Harford County, Maryland
Homeless Management Information System Policies and Procedures

June 2013

HARFORD COUNTY, MARYLAND
DEPARTMENT OF COMMUNITY SERVICES

319 S. Main St.
Bel Air, MD 21014
410-638-3389

Table of Contents

INTRODUCTION

The Harford County HMIS Project is a countywide implementation of a Homeless Management Information System (HMIS) and is administered by the Harford County Department of Community Services. Bowman Internet Systems, Inc. (BIS) provides the data base program, hosts Harford County's database and provides technical assistance to HC HMIS staff. The project utilizes Internet-based technology to assist homeless service organizations across Harford County to capture information about the clients that they serve. HC HMIS staff provides training and technical assistance (with BIS support) to users of the system throughout Harford County.

Goals of the HC HMIS Project are to enhance service coordination for homeless clients, enable services providers to measure the effectiveness of their interventions, facilitate Harford County Continuum of Care (HC CoC) analysis of service needs and gaps, thereby informing public officials and policy makers about the extent and nature of homelessness in Harford County. This is accomplished through analysis and release of data that are grounded in the actual experiences of homeless persons and the service providers who assist them in shelters and homeless assistance programs throughout the state. Information that is gathered via interviews, conducted by service providers with clients, is analyzed for an unduplicated count, aggregated (void of any identifying client level information) and made available to public officials, HC CoC service providers, and clients.

The HC HMIS project is advised by a broad-based steering committee committed to understanding the gaps in services to consumers of the human service delivery system in an attempt to end homelessness. This group is committed to balancing the interests and needs of all stakeholders involved: homeless men, women, and children; service providers; and public officials and policy makers.

Potential benefits for homeless men, women, and children and case managers: Case managers can use the software as they assess their clients' needs to inform clients about services offered on site or available through referral. Case managers and clients can use on-line resource information to learn about resources that help clients find and keep permanent housing or meet other goals clients have for themselves. Service coordination can be improved when information is shared among case management staff within one agency or with staff in other agencies (with written client consent) who are serving the same clients. When client histories are shared, the number of times the client must "tell their story" is reduced.

Potential benefits for agency and program managers: The system provides real-time information about the needs and available services for homeless persons, tracks client outcomes and provides a client history and facilitates the coordination of services internally and externally with other agencies and programs. When aggregated, information can be used to garner a more complete understanding of clients' needs and outcomes, and then used to advocate for additional resources, complete grant applications, conduct evaluations of program services, and report to funders such as DHR and HUD. The software has the capability to generate the HUD Annual Progress Report (APR).

Potential benefits for Harford County: Utilizing aggregate data generated through the HMIS, Harford County and the Harford Roundtable we will be: better able to define and understand the extent of homelessness in the county, better able to focus staff and financial resources to those geographic areas, agencies and programs where services for homeless persons are needed most, better able to evaluate the effectiveness of specific interventions and specific programs and services provided, better able to provide local, state and federal officials with information on homelessness in Harford County, better able to meet all federal, state and local reporting requirements.

Governing Principles

This document provides the policies, procedures, guidelines, and standards that govern the HC HMIS project, as well as roles and responsibilities for HC HMIS, Bowman Internet Systems and participating agency staff. Described below are the overall governing principles upon which all other decisions pertaining to the HC HMIS project are based.

Data Integrity: Data are the most valuable assets of the HC HMIS Project. It is our policy to protect this asset from accidental or intentional unauthorized modification, disclosure, or destruction.

Access to Client Records: The Client Records Access policy is designed to protect against the recording of information in unauthorized locations or systems. Only staff that work directly with clients or who have administrative responsibilities will receive authorization to look at, enter, or edit client records. Additional privacy protection policies include:

- No client records will be shared manually or electronically with another agency without written client consent
- Client has the right to refuse to answer any question, unless entry into a service program requires it
- Client has the right to know who has viewed, added to, deleted, or edited their client record
- Client information transferred from one authorized location to another over the web is transmitted through a secure, encrypted connection

Computer Crime: Computer crimes violate state and federal law as well as the HC HMIS Data Security Policy and Standards. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs, or hardware; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data, or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both. HC HMIS staff and authorized agencies must comply with license agreements for copyrighted software and documentation. Licensed software must not be copied unless the license agreement specifically provides for it. Copyrighted software must not be loaded or used on systems for which it is not licensed.

End User Ethics: Any deliberate action that adversely affects the resources of any participating organization or institution or employees is prohibited. Any deliberate action that adversely affects any individual is prohibited. Users should not use HC HMIS computing resources for personal purposes. Users must not attempt to gain physical or logical access to data or systems for which they are not authorized. Users must not attempt to reverse-engineer commercial software. Users must not load unauthorized programs or data onto HC HMIS computer systems. Users should scan all personal computer programs and data for viruses before logging onto HC HMIS computer systems.

SECTION 1:
Contractual Requirements and Roles

P&P#: CRR 1.1	**Revision:**	**Prepared by: HC HMIS**
Effective date:	**Revision date:**	**Revised by:**

HC HMIS Contract Requirements

Policy: HC HMIS is committed to provide services to participating agencies.

Standard: HC HMIS will provide quality service to existing and new participating agencies.

Purpose: To outline the basic services for existing and new agencies

Scope: Participating agencies and HC HMIS Project

Basic Requirements:

A. Purchase of Software Licensing and Technical Support: As long as funding is available, l existing sites participating in the HC HMIS Project that are funded through the Harford County, will have most costs for participation in HC HMIS covered under their current contracts. These costs include user licenses for ServicePoint and technical assistance provided by HC HMIS staff. If funds for the HC HMIS are decreased, changed, or discontinued, service providers utilizing the system will be notified. Mandates for the continued utilization of the HMIS in order to receive government funding will be outlined in the notice. Please note: Participating Agencies are responsible for all costs associated with hardware acquisition and maintenance, personnel, and Internet access. Additional licenses maybe purchased at each agency's expense.

Agencies that are not funded to participate in the HC HMIS Project through a Harford County

must pay a yearly fee according to the HC HMIS cost document.

B. Access: Existing and new Participating Agencies covered under existing Contacts will not be granted access to the ServicePoint software system until a contractual agreement has been signed with HC HMIS.

P&P#: CRR 1.2	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Steering Committee

Policy: A Steering Committee, representing all stakeholders to this project will advise project activities.

Standard: The responsibilities of the Steering Committee will be apportioned according to the information provided below.

Purpose: To define the roles and responsibilities of the project Steering Committee.

Scope: All project stakeholders

Responsibilities:

The Steering Committee advises and supports HC HMIS' operations in the following programmatic areas: resource development; consumer involvement; and quality assurance/accountability. The committee meets quarterly.

Membership of the Steering Committee will be established according to the following guidelines:

- The HC HMIS Steering Committee is fundamentally an advisory committee to the HC HMIS project. The Steering Committee assists in developing, reviewing and providing feedback on HMIS Policy and Procedure drafts. Some key issues include:

  - Assisting in the development of the guiding principles that should underlie the implementation activities of HC HMIS and participating organizations and service programs;

  - Selecting the minimal data elements to be collected by all programs participating in the HC HMIS project;

  - Reviewing and providing feedback on the criteria, standards, and parameters for the release of aggregate data; and

  - Reviewing privacy protection provisions in project implementation and operation.

- Target for membership will be 5 persons;

- There will be a pro-active effort to fill gaps in the membership of the Committee in terms of constituency representation: consumer representatives, shelters and housing programs for both families and individuals, and government agencies that fund homeless assistance services, and countywide geographic distribution.

P&P#: CRR 1.3	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

HC HMIS Management

Policy: An HC HMIS staff is in place to support the operations of the HC HMIS countywide system according to the Guiding Principles described in the Introduction.

Standard: The responsibilities of the HC HMIS staff will be assigned according to the information provided below.

Purpose: To define the roles and responsibilities of the HC HMIS staff.

Scope: System wide

HC HMIS Roles and Responsibilities:

System Management:

The HC HMIS staff is responsible for oversight of all day-to-day operations including: technical infrastructure; planning, scheduling, and meeting project objectives.

Technical Assistance:

The HC HMIS staff is responsible for overseeing usage of the application ServicePoint and being available for phone support as needed.

Responsibilities and Duties include:

- Provide training on a monthly basis to agency staff
- Provide technical assistance and troubleshooting as needed
- Provide technical assistance in generating funder-required reports

Data Analysis:

HC HMIS staff is responsible for the following:

- Provide data quality queries to sites on a regular basis.
- Provide detailed countywide reports on families and individuals accessing emergency shelter.

Systems Administration / Security / User Accounts:

- HC HMIS has a contract with Bowman Internet Systems to host the central server. BIS will have overall responsibility for the security of the system.
- HC HMIS will review all network and security logs regularly.
- All Agency Administrator user accounts are the responsibility of the HC HMIS staff. All Agency staff user accounts are the responsibility of the Agency Administrator.

P&P#: CRR 1.4	**Revision: 1**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date: 09/04**	**Revised by: HC HMIS**

HC HMIS Management (HC HMIS Administrator) Security and Confidentiality Requirements

Policy: HC HMIS System Administrators will take all necessary steps to safe guard all client information and keep confidential all identifying client data.

Standard: At no time will client-identifying data be released to anyone without a written, signed release from the individual involved.

Purpose: To outline the procedures required of HC HMIS System Administrators

Scope: System Administrators

HC HMIS Roles and Responsibilities:

HC HMIS' role is to collect data through the HMIS to be used only for CoC planning, reporting, evaluation as well as for program reporting, monitoring, evaluation, staff training and data quality monitoring and are not to be released to any party other than HC HMIS Project Staff, Community Development Review Board members and Participating Agencies. Any information received from the HC HMIS Project will be completely stripped of identifying information about the client's entered into the HC HMIS database. All reports will be produced using only client ID numbers (not names) to assure that all reporting information is de-identified.

The HC HMIS staff will not view any client identifying information about an agency's data. If a problem arises at a site that requires me to view client identified information, the Agency Administrator will log onto the ServicePoint system from his/her designated location and I will advise the Agency Administrator as to the steps to resolve the problem from their site location. HC HMIS staff members are obligated to hold all information that I learn about clients as confidential.

Any unauthorized copying or dissemination of all or a portion of the HC HMIS client identifiable data is punishable by termination of employment; and may result in severe civil and criminal penalties and will be punishable to the maximum extent possible under the law.

Business Associate Agreements for Confidentiality of Client Health Information

- Harford County, Maryland will enter into a Business Associate Agreement with each Participating Agency in the Harford County HMIS.
- HC HMIS Systems Administrators will adhere to all requirements of the Business Associate Agreements signed with each Participating Agency.

HC HMIS Staff Security and Confidentiality Commitment Agreement

- All HC HMIS staff will sign the HC HMIS Staff Commitment Agreement. See Attachment A.11.

P&P#: CRR 1.5	**Revision:**	**Prepared by: HC**
HMIS Effective date: 05/04	**Revision date:**	**Revised by:**

BIS / Harford County, End User and Taxonomy Agreements

Policy: HC HMIS staff and all Participating Agency staff will abide by the contractual agreement with Bowman Internet Systems (BIS) regarding trade secret confidentiality and Taxonomy Index confidentiality

Standard: Contract compliance

Purpose: Contract Compliance

Scope: System wide

Procedures:

BIS / Harford County Agreement

Comply with all elements of this agreement. See attachment 2.

End User Agreement

Comply with all elements of this agreement. See attachment 3.

Taxonomy Use Agreement

Comply with all elements of this agreement as stated in the End User Agreement.

See attachment 3

Homeless Management Information System (HMIS) Data and Technical Standards Final Notice

See attachment 4

Business Associate Agreement

All Agency Directors must sign and comply with all elements of a Business Associate Agreement with Harford County Government. See attachment 5.

User License Policy, Responsibility & Confidentiality Statement

All Agency Directors and Agency Staff End Users must sign and comply with all elements of

User License Policy, Responsibility, and Confidentiality Statement. See attachment 6.

P&P#: CRR 1.6	**Revision: 1**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date: 09/04**	**Revised by: HC HMIS**

Role: Participating Agency Executive Director

Policy: The Executive Director of each Participating Agency will be responsible for oversight of all agency staff that generate or have access to client-level data stored in the system software to ensure adherence to the HC HMIS standard operating procedures outlined in this document.

Standard: The Executive Director holds final responsibility for the adherence of his/her agency's personnel to the HC HMIS Guiding Principles and Standard Operating Procedures outlined in this document.

Purpose: To outline the role of the agency Executive Director, with respect to oversight of agency personnel in the protection of client data within the system software application.

Scope: Executive Director in each Participating Agency

Responsibilities:

The Participating Agency's Executive Director is responsible for all activity associated with agency staff access and use of the ServicePoint data system. This person is responsible for establishing and monitoring agency procedures that meet the criteria for access to the ServicePoint Software system, as detailed in the Policies and Procedures outlined in this document. The Executive Director will be held liable for any misuse of the software system by his/her designated staff. The Executive Director agrees to allow access to the ServicePoint software system based upon need. Need exists only for those shelter staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients, do data entry or who have agency or HMIS administration responsibilities.

The Executive Director also oversees the implementation of data security policies and standards and will:

1. Require all agency end users (agency staff persons) to sign the Harford County HMIS Agency Agreement and the User License Policies, Responsibilities and Confidentiality Statements and forward a copy with an original signature to Harford County Dept. of Community Services, HMIS Project, 319 S. Main St., Bel Air, MD 21014.

2. Assume responsibility for integrity and protection of client-level data entered into the ServicePoint system;

3. Establish business controls and practices to ensure organizational adherence to the HC HMIS Policies and Procedures;

4. Communicate control and protection requirements to agency custodians and users;

5. Authorize data access to agency staff and assign responsibility for custody of the data;
6. Monitor compliance and periodically review control decisions.
7. Assure the development and posting of an agency Privacy Notice to clients

P&P#: CRR 1.7	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Participating Agency Administrator

Policy: Every Participating Agency must designate one person to be the Agency Administrator.

Standard: The designated Agency Administrator holds responsibility for the administration of the system software in his/her agency.

Purpose: To outline the role of the Agency Administrator

Scope: Participating Agencies

Responsibilities:

The Participating Agency agrees to appoint one person as the Agency Administrator. This person will be responsible for:

- Editing and updating agency information
- Granting technical access to the software system for persons authorized by the agency's Executive Director by creating usernames and passwords;
- Training new staff persons on the uses of the ServicePoint software system including review of the Policies and Procedures in this document and any agency policies which impact the security and integrity of client information as well as assuring that they have signed the Harford County HMIS Agency Agreement.
- Ensuring that access to the ServicePoint system be granted to authorized staff members only after they have received training and satisfactorily demonstrated proficiency in use of the software and understanding of the Policies and Procedures and agency policies referred to above.
- Notifying all users in their agency of interruptions in service

The Agency Administrator is also responsible for implementation of data security policy and standards, including:

- Administering agency-specified business and data protection controls
- Administering and monitoring access control
- Providing assistance in the backup and recovery of data
- Detecting and responding to violations of the Policies and Procedures or agency procedures.

P&P#: CRR 1.8	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

User

Policy: All individuals at the HC HMIS and at the Participating Agency levels who require legitimate access to the software system will be granted such access.

Standard: Individuals with specific authorization can access the system software application for the purpose of conducting data management tasks associated with their area of responsibility.

Purpose: To outline the role and responsibilities of the system user.

Scope: System wide

Responsibilities:

HC HMIS agrees to authorize use of the ServicePoint Software system only to users who need access to the system to enter client information into the system, access community resources information and make referrals, check clients into the shelter/program, assess and document client needs, identify services for which they are eligible, develop and record case plan information and progress, shelter/program check-out information and follow-up.

The **Participating Agency** agrees to authorize use of the ServicePoint Software system only to users who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities.

Users are any persons who use the ServicePoint software for data processing services. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with the data security policy and standards as described in these Policies and Procedures. Users must sign the Harford County HMIS Agency Agreement attesting that they will follow all HC HMIS Policies and Procedures. They are accountable for their actions and for any actions undertaken with their usernames and passwords.

SECTION 2:
Participation Requirements

P&P#: CRR 2.1	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date: 09/04**	**Revised by: HC HMIS**

Participation Requirements

Many of the policies in this section concern privacy and confidentiality issues. Terms not normally used in daily conversation are included and may need explanation. Key terms are defined below.

Definition of Terms

1. *Protected Personal Information (PPI)*. Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

2. *Covered Homeless Organization (CHO)*/Participating Agency. Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes PPI on homeless clients for an HMIS.

3. *Processing*. Any operation or set of operations performed on PPI, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission and destruction of the information.

4. *HMIS Uses and Disclosures*. The uses and disclosures of PPI that are allowed by these standards.

Participation Requirements cont'd

Policy: HC HMIS staff will communicate requirements for participation. All requirements for participation are outlined in this document.

Standard: HC HMIS staff and Participating Agencies will work to ensure that all sites receive the benefits of the system while complying with all stated policies.

Purpose: To provide the structure of on-site support and compliance expectations.

Scope: System wide

Procedure: Participation Agreement Requirements

- **High Speed Internet Connection Greater than 56k/v90:** DSL, Cable, etc.

- **Identification of Agency Administrator:** Designation of one key staff person to serve as Agency Administrator. This person will be responsible for creating usernames and passwords and monitoring software access. This person will also be responsible for training new staff persons on how to use the ServicePoint system.
- **Security Assessment:** Meeting of Agency Executive Director (or designee), Program Manager/Administrator and Agency Administrator with HC HMIS staff member to assess and complete Agency Information Security Protocols. See attached Initial Implementation Requirements.
- **Training:** Commitment of Agency Administrator and designated staff persons to attend training(s) prior to accessing the system online. **Note**: Staff will **NOT** be allowed to attend training until **ALL** Information Security paperwork is complete and signed by Executive Director (or designee).
- **Interagency Data Sharing Agreements**: Interagency Data Sharing Agreements must be established between any shelter/service program where sharing of client level information is to take place. See attached Interagency Data Sharing Agreement.
- **Client Consent Forms** must be created for clients to authorize the sharing of their personal information electronically with other Participating Agencies through the ServicePoint software system where applicable. See attached Client Consent Form as an example.

- **Client Privacy Notice Statement** must be developed, posted and available to clients upon request.
- **Participation Agreement:** Agencies are required to sign a participation agreement stating their commitment to develop the policies and procedures for effective use of the system and proper collaboration with HC HMIS. See attached Initial Implementation Requirements.
- **Minimal Data Elements:** Agencies will be required to enter minimal data elements as defined by the Harford County Department of Community Services.

P&P#:PR 2.2	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Implementation Requirements

Policy: All Participating Agencies must read and understand all participation requirements and complete all required documentation prior to implementation of the system.

Standard: All implementation requirements must be complete and on file prior to using the system.

Purpose: To indicate documentation requirements prior to implementation.

Scope: Participating Agencies

Procedure: HC HMIS Server staff will assist Participating Agencies in the completion of all required documentation.

On Site Security Assessment Meeting: Meeting of Agency Executive Director or authorized designee, Program Manager/Administrator and Agency Administrator with HC HMIS staff member to assist in completion of the Agencies' Information Security Protocols.

Participation Agreement – Harford County HMIS Agency/End User Agreement

The Participating Agreement refers to the document agreement made between the participating agency and the HC HMIS project. This agreement includes commitment to minimal data as defined by the HC HMIS Project and its Steering Committee on all clients. This document is the legally binding document that refers to all laws relating to privacy protections and information sharing of client specific information. See attached Initial Implementation Requirements.

Agency Participation/Data Sharing Agreements: Upon completion of the Security Assessment, each agency must agree to abide by all policies and procedures laid out in the HC HMIS Security Manual. The Executive Director or designee will be responsible for signing this form. See attached Initial Implementation Requirements.

Identification of Referral Agencies: ServicePoint provides a resource directory component that tracks service referrals for clients. Each Participating Agency must compile a list of referral agencies and verify that the information has been entered into ResourcePoint.

HC HMIC User License Policy, Responsibility, and Confidentiality Statements: All agency staff persons must comply with these statements. See attachment 6.

P&P#:PR 2.3	**Revision:**	**Prepared by: HC HMIS**
Effective date: 09/04	**Revision date:**	**Revised by:**

HIPAA Precedence over HMIS Privacy Standards for PPI

Policy: Any CHO that is covered under the HIPAA is not required to comply with the privacy or security standards in this Notice.

Standard: Any CHO that is covered under the HIPAA is not required to comply with the privacy or security standards in this Notice if the CHO determines that a substantial portion of its PPI about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules.

Purpose: Exempting HIPAA covered entities from the HMIS privacy and security rules avoids all possible conflicts between the two sets of rules. The HMIS standards give precedence to the HIPAA privacy and security rules because: (1) The HIPAA rules are more finely attuned to the requirements of the health care system; (2) the HIPAA rules provide important privacy and security protections for protected health information; and (3) requiring a homeless provider to comply with or reconcile two sets of rules would be an unreasonable burden.

Scope: Homeless Organizations covered by HIPAA.

Procedure: Homeless Organizations covered by HIPAA should comply with HIPAA regulations as pertaining to the privacy and security of client PPI. Covered Health Care Organizations must, however, comply with all other policies and procedures included in this manual. These include but are not limited to implementation protocols, required agreements, confidentiality statements, adherence to contractual requirements, training requirements, etc.

P&P#:PR 2.4	**Revision:**	**Prepared by: HC HMIS**
Effective date: 09/04	**Revision date:**	**Revised by:**

Allowable HMIS Uses and Disclosures of PPI

Definition of Terms

1. *Protected Personal Information (PPI).* Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

2. *Covered Homeless Organization (CHO)*/Participating Agencies. Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes PPI on homeless clients for an HMIS.

3. *Processing.* Any operation or set of operations performed on PPI, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission and destruction of the information.

4. *HMIS Uses and Disclosures*. The uses and disclosures of PPI that are allowed by these standards.

Policy: A CHO may use or disclose PPI from an HMIS under the following circumstances: (1) To provide or coordinate services to an individual; (2) for functions related to payment or reimbursement for services; (3) to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or (4) to create de-identified PPI.

Standard: CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of clients. The following additional uses and disclosures recognize those obligations to use or share personal information by balancing competing interests in a responsible and limited way. Under the HMIS privacy standard, these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this standard modifies an obligation under applicable law to use or disclose personal information.

Purpose: To document appropriate uses and disclosures of PPI.

Scope: These privacy standards apply to any homeless assistance organization that records, uses or processes protected personal information (PPI) for an HMIS. A provider that meets this definition is referred to as a covered homeless organization (CHO). All PPI maintained by a CHO is subject to these standards. Any CHO that is covered under the HIPAA is not required to comply with the privacy or security standards in this Notice if the CHO determines that a substantial portion of its PPI about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules.

Procedure: *Uses and disclosures required by law*. A CHO may use or disclose PPI

when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

Uses and disclosures to avert a serious threat to health or safety. A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PPI if: (1) The CHO, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

Uses and disclosures about victims of abuse, neglect or domestic violence. A CHO may disclose PPI about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence under any of the following circumstances:

. • Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;

. • If the individual agrees to the disclosure; or

. • To the extent that the disclosure is expressly authorized by statute or regulation; and the CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:

. • The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

• The CHO would be informing a personal representative (such as a family member or friend), and the CHO reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the CHO, in the exercise of professional judgment.

Uses and disclosures for academic research purposes. A CHO may use or disclose PPI for academic research conducted by an individual or institution that has a formal relationship with the CHO if the research is conducted either:

. • By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the CHO; or

• By an institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the CHO.

ALLOWABLE HMIS USES AND DISCLOSURES OF PPI - *continued*

A written research agreement must:

(1) Establish rules and limitations for the processing and security of PPI in the course of the research;

(2) Provide for the return or proper disposal of all PPI at the conclusion of the research;

(3) Restrict additional use or disclosure of PPI, except where required by law; and

(4) Require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

Disclosures for law enforcement purposes. A CHO may, consistent with applicable law and standards of ethical conduct, disclose PPI for a law enforcement purpose to a law enforcement official under any of the following circumstances:

• In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;

. • If the law enforcement official makes a written request for protected personal information that: (1) Is signed by a supervisory official of the law enforcement agency seeking the PPI; (2) states that the information is relevant and material to a legitimate law enforcement investigation; (3) identifies the PPI sought; (4) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (5) states that de-identified information could not be used to accomplish the purpose of the disclosure.

. • If the CHO believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of the CHO;

. • In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; or

. • If (1) the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22

U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and (2) the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

P&P #:PR 2.5	**Revision:**	**Prepared by: HC HMIS**
Effective date: 09/04	**Revision date:**	**Revised by:**

HMIS Privacy Standards and Collection Limitations for Agencies Recording PPI

Policy: All CHOs must protect the privacy of all identifiable PPI. Privacy protections must be described in the CHO's privacy notice. A CHO must comply with all baseline privacy protections and with all additional privacy protections included in its privacy notice. A CHO may collect PPI only when appropriate to the purposes for which the information is obtained or when required by law.

Standard: All CHOs must comply with the baseline privacy requirements described here with respect to: data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. A CHO may adopt additional substantive and procedural privacy protections that exceed the baseline requirements for each of these areas. A CHO must comply with federal, state and local laws that require additional confidentiality protections. All additional protections must be described in the CHO's privacy notice. A CHO must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.

Purpose: To ensure the confidentiality of identifiable PPI.

Scope: A CHO must comply with all baseline privacy protections and with all additional privacy protections included in its privacy notice. A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PPI. When PPI is shared between organizations, responsibilities for privacy and security may reasonably be allocated between the organizations. Organizations sharing a common data storage medium and PPI may adopt differing privacy and security policies as they deem appropriate, administratively feasible, and consistent with these HMIS privacy and security standards, as long as these privacy and security policies allow for the de-duplication of homeless clients at the CoC level.

Procedure: A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information. Consent of the individual for data collection may be inferred from the circumstances of the collection. Providers may use the following language to meet this standard: ''we collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.''

Optional Additional Privacy Protections. A CHO may, in its privacy notice, commit to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Restricting collection of personal data, other than required HMIS data elements;

(2) Collecting PPI only with the express knowledge or consent of the individual (unless required by law); and

(3) Obtaining oral or written consent from the individual for the collection of personal information from the individual or from a third party.

P&P #:PR 2.6	**Revision:**	**Prepared by: HC HMIS**
Effective date: 09/04	**Revision date:**	**Revised by:**

Client Notification of Purpose of Collecting PPI and the Use and Disclosure of PPI

Policy: All CHOs must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures.

Standard: A CHO may use or disclose PPI only if the use or disclosure is allowed by this standard and is described in its privacy notice. A CHO may infer consent for all uses and disclosures specified in the notice and for uses and disclosures determined by the CHO to be compatible with those specified in the notice.

Purpose: To ensure client awareness of CHO's purpose for collecting data, the ways in which it will be used and to whom it is disclosed.

Scope: All CHOs using HC HMIS.

Procedure: All CHOs must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures. A CHO may use or disclose PPI only if the use or disclosure is allowed by this standard and is described in its privacy notice. A CHO may infer consent for all uses and disclosures specified in the notice and for uses and disclosures determined by the CHO to be compatible with those specified in the notice. Except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law.

Optional Additional Privacy Protections. A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Seeking either oral or written consent for some or all processing when individual consent for a use, disclosure or other form of processing is appropriate;

(2) Agreeing to additional restrictions on use or disclosure of an individual's PPI at the request of the individual if the request is reasonable. The CHO is bound by the agreement, except if inconsistent with legal requirements;

(3) Limiting uses and disclosures to those specified in its privacy notice and to other uses and disclosures that are necessary for those specified;

(4) Committing that PPI may not be disclosed directly or indirectly to any government agency (including a contractor or grantee of an agency) for inclusion in any national homeless database that contains personal protected information unless required by statute;

(5) Committing to maintain an audit trail containing the date, purpose, and recipient of some or all disclosures of PPI;

(6) Committing to make audit trails of disclosures available to the homeless individual; and

(7) Limiting disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure.

P&P #:PR 2.7	**Revision:**	**Prepared by: HC HMIS**
Effective date: 09/04	**Revision date:**	**Revised by:**

Client Notification of HMIS Privacy Standards for Agencies Recording PPI

Policy: A CHO must publish a privacy notice describing its polices and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request.

Standard: A CHO must publish a privacy notice describing its polices and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page. A CHO may, if appropriate, omit its street address from its privacy notice. A CHO must post a sign stating the availability of its privacy notice to any individual who requests a copy.

Purpose: To ensure client awareness of CHO's privacy policies and procedures for the processing of PPI.

Scope: All CHOs using HC HMIS.

Procedure: A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. All amendments to the privacy notice must be consistent with the requirements of these privacy standards. A CHO must maintain permanent documentation of all privacy notice amendments.

CHOs are reminded that they are obligated to provide reasonable accommodations for persons with disabilities throughout the data collection process. This may include but is not limited to, providing qualified sign language interpreters, readers or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability. *See* 24 CFR 8.6; 28 CFR 36.303. **Note:** This obligation does not apply to CHOs who do not receive federal financial assistance and who are also exempt from the requirements of Title III of the Americans with Disabilities Act because they qualify as ''religious entities'' under that Act.

In addition, CHOs that are recipients of federal financial assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the program. *See HUD Limited English Proficiency Recipient Guidance* published on December 18, 2003 (68 FR 70968).

Optional Additional Privacy Protections. A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) making a reasonable effort to offer a copy of the privacy notice to each client at or around the time of data collection or at another appropriate time;

(2) giving a copy of its privacy notice to each client on or about the time of first data collection. If the first contact is over the telephone, the privacy notice may be provided at the first in-person contact (or by mail, if requested); and/ or

(3) adopting a policy for changing its privacy notice that includes advance notice of the change, consideration of public comments, and prospective application of changes.

P&P #:PR 2.8	**Revision:**	**Prepared by: HC HMIS**
Effective date: 09/04	**Revision date:**	**Revised by:**

Client Access to PPI Records and Corrections of Inaccurate or Incomplete Data

Policy: A CHO must allow an individual to inspect, have a copy of, and offer to explain any information collected through the HMIS. A CHO must also consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual.

Standard: A CHO must allow an individual to access to the data (specific to the client) that is stored in the system. Clients must be provided with a copy of their records if requested and a CHO must offer to explain any information that the individual may not understand. A CHO must consider any request by an individual for correction of inaccurate or incomplete PPI in their file.

Purpose: To ensure client access to and input on PPI recorded about them by the CHO

Scope: All CHOs using HC HMIS.

Procedure: A CHO must allow an individual to inspect, have a copy of, and offer to explain any information collected through the HMIS. A CHO must also consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

In its privacy notice, a CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PPI:

(1) Information compiled in reasonable anticipation of litigation or comparable proceedings;

(2) information about another individual (other than a health care or homeless provider);

(3) information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or

(4) information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

A CHO can reject repeated or harassing requests for access or correction. A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

Optional Additional Privacy Protections. A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Accepting an appeal of a denial of access or correction by adopting its own appeal

procedure and describing the procedure in its privacy notice;

(2) Limiting the grounds for denial of access by not stating a recognized basis for denial in its privacy notice;

(3) Allowing an individual whose request for correction has been denied to add to the individual's information a concise statement of disagreement. A CHO may agree to disclose the statement of disagreement whenever it discloses the disputed PPI to another person. These procedures must be described in the CHO's privacy notice; and/or

(4) Providing to an individual a written explanation of the reason for a denial of an individual's request for access or correction.

P&P #:PR 2.9	**Revision:**	**Prepared by: HC HMIS**
Effective date: 09/04	**Revision date:**	**Revised by:**

CHO Accountability for Client Access to PPI Records and Corrections of Data

Policy: A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices.

Standard: A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors, and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

Purpose: To ensure client access to and input on PPI recorded about them by the CHO

Scope: All CHOs using HC HMIS.

Procedure: A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors, and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

Optional Additional Privacy Protections. A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Requiring each member of its staff (including employees, volunteers, affiliates, contractors, and associates) to undergo (annually or otherwise) formal training in privacy requirements;

(2) Establishing a method, such as an internal audit, for regularly reviewing compliance with its privacy policy;

(3) Establishing an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of a denial of access or correction rights; and/or

(4) Designating a chief privacy officer to supervise implementation of the CHO's privacy standards.

P&P#: PR 2.10	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Interagency Data Sharing Agreements

Policy: Data sharing among agencies will be supported upon completion of Interagency Sharing Agreements by Participating Agencies wishing to share client-identified data.

Standard: For participating agencies to engage in data sharing arrangements, a written, formal document must be signed by the Executive Directors of each of the Participating Agencies involved in the data sharing.

Purpose: To explain the vehicle through which agencies can enter into an agreement allowing them to share client records.

Scope: Participating Agencies wishing to share client records.

Responsibilities:

Interagency Sharing Agreements

A. Written Agreement: Participating Agencies wishing to share information electronically through the ServicePoint System are required to provide, in writing, an agreement that has been signed between the Executive Directors of Participation Agencies. See attached Interagency Sharing Agreement.

B. Role of Executive Director: The Executive Director is responsible for abiding by all the policies stated in any Interagency Sharing Agreement.

Procedure:

A. Executive Directors wishing to participate in a data sharing agreement contact HC HMIS staff to initiate the process.

B. Executive Directors complete the Interagency Sharing Agreement. Each participating agency retains a copy of the agreement and a master is filed with the HC HMIS Organization.

C. Agency Administrators receive training on the technical configuration to allow data sharing.

D. Each Client whose record is being shared must agree via a written client consent form to have their data shared. A client must be informed what information is being shared and with whom it is being shared.

P&P#: PR 2.11	**Revision:**	**Prepared by: HC**
HMIS Effective date: 05/04	**Revision date:**	**Revised by:**

Written Client Consent Procedure for Electronic Data Sharing

Policy: As part of the implementation strategy of the system software, a Participating Agency must have client consent procedures and completed forms in place when electronic data sharing is to take place.

Standard: Client consent procedures must be on file prior to the assignment of user accounts to the site by HC HMIS staff.

Purpose: To indicate the type of client consent procedures that Participating Agencies must implement prior to actual implementation.

Scope: Participating Agencies wishing to share client records

Procedure:

Client Consent Procedures

See Attachment A.13 Sample Client Consent Form.

P&P#: PR 2.12	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Confidentiality and Informed Consent

Policy: All Participating Agencies agree to develop an oral explanation of the HMIS system and their Agency's Privacy notice. Agencies may choose to commit their Agency staff to securing a signed client release of information before entering information into the HMIS.

Standard: Agencies must also develop procedures for providing oral explanations to clients about the usage of the computerized Homeless Management Information System. Participating Agencies are may also require the use of written client consent forms when entering client PPI into the HMIS. A client release must be signed when specific information is to be shared with another agency.

Purpose: To ensure protection of clients' privacy.

Scope: Participating Agencies

Procedure: Confidentiality/ Client Consent

Informed Consent: Oral Explanation (non-shared records): All Agencies must provide an oral explanation about the HMIS system, their Agency's privacy notice as well as the uses and disclosures of PPI. Clients who do not give their consent will not be denied services.

HC HMIS suggests including the following information in the oral explanation and on the fact sheet:

1. What ServicePoint is

- A web-based information system that homeless services agencies across the County use to capture information about the persons they serve

2. Why the agency uses it

- to understand their clients' needs
- help the programs plan to have appropriate resources for the people they serve
- to inform public policy
- two persons at Harford County government, the Harford County HMIS System Administrators, will have access to client data. These two people will never enter a

client file unless a client-authorized person from the service agency requests assistance on how to enter data into the system. Client-authorized Participating Agency personnel or individual clients with proof of identity may request an Audit Report showing all persons who viewed the client's file and any changes made to the file. To make a request, contact the Harford County Community Development Administrator of Community Services or the System Administrators at 319 S. Main St., Bel Air, 410-638-3389 during normal business hours.

The System Administrators will also run monthly reports that total the number of people served in the CoC that month, aggregate (aggregate means summary statistics - no individual client data) reports on the services that clients need/receive and other reports that help assure appropriate services are delivered to clients and/or to assist the Harford County CoC to identify service gaps and create services that meet client needs. The System Administrators must also provide aggregate data reports for funding sources that pay for client services.

3. Security

- Only staff that work directly with clients or who have administrative responsibilities can look at, enter, or edit client records

4. Privacy Protection

- No information will be released to another agency or person without written client consent
- Client has the right to not answer any in the HMIS assessments question, unless entry into a program requires it

  Client has the right to know who has viewed added to, deleted, or edited their ServicePoint record. To request a client file Audit Report, the client or a client-authorized person from the service agency, may contact the Harford County Administrator of Community Services or the System Administrator II at 410-638-3389 during normal business hours.
- Information that is transferred over the web is through a secure connection

5. Benefits for clients

- Case manager tells client what services are offered on site or by referral through the assessment process
- Case manager and client can use information to assist clients in obtaining resources that will help them meet their needs.

Information Release: The all Participating Agencies, including the HMIS System Administrators, agree not to release client identifiable information to any other person or organization pursuant to federal and state law without proper client consent. Each Participating Agency must develop a written client consent form. A sample form is included in this document as Attachment 13.

Federal/State Confidentiality Regulations: The participating Agency will uphold Federal and State Confidentiality regulations to protect client records and privacy. In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in the regulations.

CONFIDENTIALITY AND INFORMED CONSENT - *continued*

1) The Participating Agency will abide specifically by the Federal confidentiality rules as contained in 42 CFR Part 2 regarding disclosure of alcohol and/or drug abuse records. In general terms, the Federal rules prohibit the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Participating Agency understands that the Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.

2) The Participating Agency will abide specifically by State of Maryland Code, Health - General, Title 4, Statistics, and Records, Subtitle 3 Confidentiality of Medical Records. In general, this law provides guidance for release of client level information including who has access to client records, for what purpose and audit trail specifications for maintaining a complete and accurate record of every access to and every use of any personal data by persons or organizations. The act requires written informed consent by the consumer for any individual or organization (whether or not they provide health care services) to re-release medical information. The act also further limits disclosure in Mental Health Records without a patient's consent to those exceptions enumerated in section 4-307.

3) For Participating Agencies not covered by HIPAA, HUD as developed Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice. This notice was published in the Federal Register on July 30, 2004 and is included in this document as Attachment 4.

P&P#: PR 2.13	**Revision: 1**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date: 03/10**	**Revised by: HC HMIS**

Minimal Data Elements

Policy: Participating Agencies that collect client data through this Homeless Management Information system will, at a minimum, collect all data needed for government reporting purposes.

Standard: All agencies will collect minimal data elements.

Purpose: To ensure that agencies are collecting uniform data.

Scope: Participating Agencies

Procedure:

Commitment to Utilization of Interview Protocol

Minimal Data Elements:

The Participating Agency is responsible for ensuring that all clients are asked a set of questions to collect data for use in aggregate analysis and for government funding reporting. Agencies may develop their own set of questions as long as all required data elements are collected. These elements are contained within the ServicePoint system in the General Demographic, Additional Profile and specialized Agency Assessments developed by HC HMIS to meet the reporting needs of government funding sources. All agencies must answer questions asked in the Client Profile screens and in the specialized Agency Assessment. Agencies that receive government funds must also complete assessments for the type of government funding that they receive. For example, Agencies that receive funding from the State of Maryland (ETHS, HPP, SLH, HWCSHP, ETC.) must complete the State of Maryland Assessment in addition to the Profile Screen and Harford County assessments. Agencies that receive Federal Emergency Shelter Grant (ESG) funding must complete the Harford County, Profile screen, and HUD ESG assessments. Agencies that receive HUD Shelter Plus Care or Supportive Housing Program funds must complete the Harford County, Profile and HUD APR assessments. Agencies that do not receive government funding must, at minimum, complete the Profile screen and the Harford County assessments.

Universal Data Elements (UDE)

1. Name
2. Social Security Number
3. Date of Birth
4. Ethnicity and Race
5. Gender
6. Veteran Status
7. Disabling Condition
8. Residence Prior to Program Entry
9. Zip Code of Last Permanent Address
10. Housing Status
11. Program Entry Date
12. Program Exit Date
13. Unique Person Identification Number
14. Program Identification Number
15. Household Identification

MINIMAL DATA ELEMENTS - *continued*

Sample questions to collect this data from clients are located in the Homeless Management Information (HMIS) Data Standards Revised Notice March 2010 (attachment 4)

Participating Agencies that provide Case Management must also collect Program Specific Data Elements.

1. Income and Sources
2. Non-Cash Benefits
3. Physical Disability
4. Developmental Disability
5. Chronic Health Condition
6. HIV/AIDS
7. Mental Health
8. Substance Abuse
9. Domestic Violence
10. Destination
11. Date of Contact
12. Date of Engagement
13. Veteran's Information
14. Services Provided
15. Financial Assistance Provided
16. Destination
17. Reasons for Leaving

Optional Data Elements In addition to the data elements that are required for APR reporting, additional program-specific data elements have been recommended by a team of HMIS practitioners, federal agency representatives, and researchers. These data elements are based on best practices. These elements are needed for the HUD APR (required reporting for S+C, SHP, SRO, SH) and for Harford County CoC reporting (required for Continuum of Care gaps and trends analysis, CoC planning and evaluation and agency reporting and evaluations).

1. Employment
2. Education
3. General Health Status
4. Pregnancy Status
5. Veteran's Information
6. Children's Education

Data elements for State of Maryland funding requirements (required reporting for ETHS, HPP, SLH, HWCSHP, etc.) as well as elements for HUD ESG reporting are included in the specialized Agency Assessments.

P&P#: PR 2.14	**Revision: 1**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date: 09/04**	**Revised by: HC HMIS**

Information Security Protocols

Policy: Participating Agencies must develop and have in place minimum information security protocols. A CHO must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, mainframes and servers. These protocols must be reviewed and approved by Harford County Community Services.

Standard: At a minimum, a Participating Agency must develop rules, protocols or

- Assignment of user accounts
- Unattended workstations
- Physical access to workstations
- Policy on user account sharing
- Client record disclosure
- Report generation, disclosure and storage

Purpose: To protect the confidentiality of the data and to ensure its integrity at the site.

Scope: Participating Agencies.

Procedures: To develop internal protocols, please reference the following regulations.

HUD Regulations – *Baseline regulations are mandatory for all CHOs/Participating Agencies.*

4.3. Security Standards

This section describes the standards for system, application, and hard copy security. All CHOs must comply with the baseline security requirements. A CHO may adopt additional security protections that exceed the baseline requirements if it chooses.

4.3.1. System Security

Applicability. Baseline Requirement. A CHO must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, mainframes and servers.

Additional Security Protections. A CHO may commit itself to additional security protections

Information Security Protocols – *continued*

consistent with HMIS requirements by applying system security provisions to all electronic and hard copy information that is not collected specifically for the HMIS. A CHO may also seek an outside organization to perform an internal security audit and certify system security.

User Authentication. Baseline Requirement. A CHO must secure HMIS systems with, at least a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

(1) Using at least one number and one letter;

(2) Not using, or including, the username, the HMIS name, or the HMIS vendor's name;

and/or

(3) Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (*e.g.*, username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

Additional Security Protections. A CHO may commit to additional security protections consistent with HMIS requirements by including one of each of the following kinds of characters in the password:

(1) upper and lower-case letters;

(2) numbers; and/or

(3) symbols.

A common solution to creating complex passwords is to use phrases instead of individual words as passwords, capitalize each new word in the phrase, and substitute numbers and symbols for letters in any given word. For example, the phrase ''secure password'' can be modified to ''$3cur3P@$$w0rd'' by replacing the letter ''s'' with ''$,'' the letter ''e'' with the number ''3,'' the letter ''a'' with ''@'' and the letter ''o'' with the number ''0,'' and eliminating spaces between words.

Virus Protection. Baseline Requirement. A CHO must protect HMIS systems from viruses by

Information Security Protocols – *continued*

using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by automatically scanning all files for viruses when the system is turned on, shut down or not actively being used.

Firewalls. Baseline Requirement. A CHO must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall as long as the server has a firewall. Firewalls are commonly included with all new operating systems. Older operating systems can be equipped with secure firewalls that are available both commercially and free on the Internet.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by applying a firewall to all HMIS workstations and systems.

Public Access. Baseline Requirement. HMIS that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure (PKI) certificates, or extranets that limit access based on the Internet Provider (IP) address, or similar means. A public forum includes systems with public access to any part of the computer through the Internet, modems, bulletin boards, public kiosks or similar arenas. Further information on these tools can be found in the HMIS Consumer Guide and the HMIS Implementation Guide, both available on HUD's Web site.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by using PKI certificates and extranets that limit access based on the IP address. A very secure system would not house any HMIS data on systems that are accessible to the general public.

Physical Access to Systems with Access to HMIS Data. Baseline Requirement. A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. Password protected screen savers are a standard feature with most operating systems and the amount of time can be regulated by a CHO. If staff from a CHO will be gone for an extended period of time, staff should log off the

data entry system and shut down the computer.

P&P #: PR 2.14	**Revision: 1**	**Prepared by: HC HMIS Effective**
Effective date: 05/04	**Revision date: 09/04**	**Revised by: HC HMIS**

Information Security Protocols – *continued*

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by automatically logging users off of the HMIS application after a period of inactivity and automatically logging users off of the system after a period of inactivity. Most server operating systems come equipped with the needed software to automatically perform these functions. If staff from a CHO will be gone for an extended period of time, staff should store the computer and data in a locked room.

Disaster Protection and Recovery. Baseline Requirement. A CHO must copy all HMIS data on a regular basis to another medium (*e.g.*, tape) and store it in a secure off-site location where the required privacy and security standards would also apply. A CHO that stores data in a central server, mini-computer or mainframe must store the central server, mini-computer or mainframe in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors must be used to protect systems used for collecting and storing all the HMIS data.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by providing, among other options, fire and water protection at the off-site location that houses the storage medium. A CHO may also seek an outside organization to conduct a disaster protection audit.

Disposal. Baseline Requirement. In order to delete all HMIS data from a data storage medium, a covered homeless organization must reformat the storage medium. A CHO should reformat the storage medium more than once before reusing or disposing the medium.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by destroying media at a bonded vendor to ensure all the HMIS data is completely destroyed.

System Monitoring. Baseline Requirement. A CHO must use appropriate methods to monitor security systems. Systems that have access to any HMIS data must maintain a user access log. Many new operating systems and web servers are equipped with access logs and some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by checking user access logs routinely for inappropriate access, hardware, and software problems, errors and viruses, or purchasing one of several software applications available that track the status of individual files on computers. These applications are used to make sure that files are not being changed when they are not supposed to be. The applications inform the system administrator if a computer has been hacked, infected with a virus, has been restarted, or if the data files have been tampered with.

P&P#: PR 2.15	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Implementation Connectivity

Policy: Participating Agencies are required to obtain an adequate Internet connection (greater than 56K/v90)

Standard: Any Internet connection greater than 56K/v90 is acceptable.

Purpose: To ensure proper response time and efficient system operation of the Internet application.

Scope: Participating Agencies

Procedure: HC HMIS staff is committed to informing all participating agencies about availability of Internet providers. Obtaining and maintaining an Internet connection greater than 56K/v90 is the responsibility of the participating agency.

P&P#: PR 2.16	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Maintenance of Onsite Computer Equipment

Policy: Participating Agencies commit to a reasonable program of data and equipment maintenance in order to sustain an efficient level of system operation.

Standard: Participating Agencies must meet the technical standards for minimum computer equipment configuration, Internet connectivity, data storage and data back up.

Purpose: To ensure that participating agencies adopt an equipment and data maintenance program.

Scope: Participating Agencies

Responsibilities:

The Executive Director or designee will be responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the HC HMIS Project including the following:

A. **Computer Equipment:** The Participating Agency is responsible for maintenance of on-site computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization in the HC HMIS Project.

B. **Backup**: The Participating Agency is responsible for supporting a backup procedure for each computer connecting to the HC HMIS Project.

C. **Internet Connection**: HC HMIS staff members are not responsible for troubleshooting problems with Internet Connections.

D. **Virus Protection**: As a matter of course, each agency should install virus protection software on all computers.

E. **Data Storage**: The Participating Agency agrees to only download and store data in a secure format.

F. Data Disposal: The Participating Agency agrees to dispose of documents that contain identifiable client level data by shredding paper records, deleting any information from diskette before disposal, and deleting any copies of client level data from the hard drive of any machine before transfer or disposal of property. HC HMIS staff is available to consult on appropriate processes for disposal of electronic client level data.

SECTION 3:

Training

P&P#: TRA 3.1	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Training Schedule

Policy: HC HMIS staff will maintain an ongoing training schedule for Participating Agencies.

Standard: HC HMIS staff will publish a schedule for trainings and will offer them regularly.

Purpose: To provide ongoing training to participating agencies.

Scope: System wide

Procedure:

A training schedule will be published on HC HMIS' website each month. Agencies must register for all trainings.

P&P#: TRA 3.2	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

User, Administrator and Security Training

Policy: All users must undergo security training before gaining access to the system. This training must include a review of HC HMIS security Policies and Procedures.

Standard: HC HMIS staff or trained Agency Administrator will provide data security training

Purpose: To ensure that staff are properly trained and knowledgeable of HC HMIS' security Policies and Procedures.

Scope: System wide

Agency staff must attend user training. Agency Administrators must also attend an Administrator training, in addition to a user training.

Procedure: Agencies will be notified of scheduled training sessions.

Training:

The Agency Administrator is responsible for training new users. Users must receive ServicePoint training prior to being granted user privileges for the system.

SECTION 4:

User, Location, Physical and Data Access

P&P#: ACC 4.1	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Access Privileges to System Software

Policy: Participating Agencies will apply the user access privilege conventions set forth in this procedure.

Standard: Allocation of user access accounts and privileges will be made according to the format specified in this procedure.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

Procedure:

User Access Privileges to ServicePoint

A. User access: User access and user access levels will be deemed by the Executive Director of the Participating Agency in consultation with the Agency Administrator. The Agency Administrator will generate username and passwords within the Administrative function of ServicePoint.

B. User name format: The Agency Administrator will create all usernames using the First Initial of First Name and Last Name. Example John Doe's username would be JDoe. In the case where there are two people with the same first initial and last name, a sequential number should be placed at the end of the above format. Ex. JDoe2, JDoe3.

C. Passwords:

1. **Creation:** Passwords are automatically generated from the system when a user is created. Site Technical Administrators will communicate the system-generated password to the user.

2. **Use of:** The user will be required to change the password the first time they log onto the system. The password must be between 8 and 16 characters and contain 2 numbers.

3. **Expiration:** Passwords expire every 45 days.

4. **Termination or Extended Leave from Employment:** The Agency Administrator should terminate the rights of a user immediately upon termination from their current position. If a staff person is to go on leave for a period of longer than 45 days, their password should be inactivated within 5 business days of the start of their leave. The Agency Administrator is responsible for removing users from the system. The Agency Administrator must update the access list and signed agreement on a quarterly basis.

P&P#: ACC 4.2	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Access Level for System Users

Policy: Participating Agencies will manage the proper designation of user accounts and will monitor account usage.

Standard: The Participating Agency agrees to apply the proper designation of user accounts and manages the use of these accounts by agency staff.

Purpose: To enforce information security protocols

Scope: Participating Agencies

Procedure: User accounts will be created and deleted by the Site Administrator under authorization of the Participating Agency's Executive Director.

Designation of Service Point Users

User Levels: There are nine (9) levels of access to the ServicePoint system. These levels should be reflective of the access a user has to client level paper records and access levels should be need-based. Need exists only for those shelter staff, volunteers, or designed personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.

Agency Access Levels

Resource Specialist I – Under this access level, a user may access only the ResourcePoint module. Users may search the database of area agencies and programs and view the agency or program detail screens. Access to client or service records and other modules and screens is not given. A resource specialist cannot modify or delete data.

Resource Specialist II – Under this access level, a user may access only the ResourcePoint module. Users may search the database of area agencies and programs and view the agency or program detail screens. Access to client or service records and other modules and screens is not given. A Resource Specialist II is an agency-level "Information & Referral (I&R) specialist" who may update their own agency and program information.

Volunteer – Under this access level, a user may access ResourcePoint, and have limited access to ClientPoint, and to service records. A volunteer may view or edit basic demographic information about clients (the profile screen), but is restricted from all other screens in ClientPoint. A volunteer may also enter new clients, make referrals, or check-in/out a client from a shelter. A volunteer does not have access to the "Services Provided" tab in HC HMIS. Normally, this access level is designed to allow a volunteer to perform basic intake steps with a new client and then refer the client to an agency

staff or case manager.

Agency Staff – Under this access level, a user may access ResourcePoint, and have full access to service records, but only limited access to ClientPoint. Agency staff may access most functions in ServicePoint, however, they may only access basic demographic data on clients (profile screen). All other screens are restricted including Reports. Agency Staff can add news items to the newswire feature of ServicePoint.

Case Manager I – Under this access level, a user may access all HC HMIS screens and modules except "Administration."A Case Manager I may access all screens within ClientPoint except, for confidentiality reasons, the medical screen. They also may access Reports.

Case Manager II – Under this access level, a user may access all HC HMIS screens and modules except "Administration." A Case Manager II may access all screens within ClientPoint, including the medical screen. They also may access Reports.

Agency Administrator – Under this access level, a user may access all ServicePoint screens and modules for their agency. This level may add/remove users and edit agency and program data for his/her agency.

Executive Director – same access rights as Agency Administrator, but ranked above Agency Administrator.

Agency Access Levels Chart

	Agency Staff	Case Manager I	Case Manager II	Resource Specialist II	Agency Administrator	Executive Director
ClientPoint						
View Client Record	x	x	x		x	x
View Inactive client record						
Modify Client Record	x	x	x		x	x
Reports						
Ability to view the reports tab and run reports	x	x	x		x	x
Client Served Report	x	x	x		x	x
Daily Unit Report	x	x	x	x	x	x
Entry Exit Report	x	x	x		x	x
Administration						
Add/edit/delete users					x	x
Modify/ delete case managers		x	x		x	x
View case managers		x	x			x
Shelterpoint	x	x	x	x	x	x

For a comprehensive list, review the help screen

https://sp5.servicept.com/harfordcounty/com.bowmansystems.sp5.core.ServicePoint/index.html

P&P#: ACC 4.3	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Location Access Privileges to System Server

Policy: Participating Agencies agree to enforce the location access privileges to the system server.

Standard: Only authorized computers will be able to access the system from authorized locations.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

Procedure:

Location Access: Access to the system software system will only be allowed from computers specifically identified by the Executive Director and Site Administrator of the Participating Agency. Those designated computers will be registered electronically with the Central Server by HC HMIS staff. Laptops and off-site installations will require an additional security form stating that use will not be for unauthorized purposes from unauthorized locations. See attached Laptop and Off-Site Installation Access Privileges to System Server Commitment Form.

P&P#: ACC 4.4	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Title: ACCESS TO DATA

Policy: Participating Agencies must agree to enforce the user access privileges to system data server as stated below.

Standard:

A. User Access: Users will only be able to view the data entered by users of their own agency. Security measures exist within the ServicePoint software system that restricts agencies from viewing each other's data.

B. Raw Data: Users who have been granted access to the ServicePoint Report Writer tool have the ability to download and save client level data onto their local computer. Once this information has been downloaded from the ServicePoint server in raw format to an agency's computer, these data then become the responsibility of the agency. A participating Agency should develop protocol regarding the handling of data downloaded from the Report Writer.

C. Agency Policies Restricting Access to Data: The Participating Agencies must establish internal access to data protocols. These policies should include who has access, for what purpose, and how they can transmit this information. Issues to be addressed include storage, transmission, and disposal of these data.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

P&P#: ACC 4.5	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Access to Client Paper Records

Policy: Participating Agencies will establish procedures to handle access to client paper records. Harford County Community Services must review and approve these procedures.

Standard: The Participating Agencies agree to establish procedures regarding which staff have access to client paper records.

Purpose: To enforce information security protocols.

Scope: Participating Agencies

Procedure:

- Identify which staff have access to the client paper records and for what purpose. Staff should only have access to records of clients that they directly work with or for data entry purposes.
- Identify how and where client paper records are stored.
- Develop policy regarding length of storage and disposal procedure of paper records.
- Develop policy on disclosure of information contained in client paper records.

P&P#: ACC 4.6	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Physical Access Control

Policy: Physical access to the system data processing areas, equipment and media must be controlled. Access must be controlled for the transportation of data processing media and other computing resources. The level of control is contingent on the level of risk and exposure to loss.

Standard: Personal computers, software, documentation and diskettes shall be secured proportionate with the threat and exposure to loss. Available precautions include equipment enclosures, lockable power switches, equipment identification and fasteners to secure the equipment.

Purpose: To delineate standards for physical access.

Scope: System wide

Guidelines:

Access to computing facilities and equipment

- The HC HMIS staff with the Administrators within Participating Agencies will determine the physical access controls appropriate for their organizational setting based on HC HMIS security policies, standards and guidelines.
- All those granted access to an area or to data are responsible for their actions. Additionally, those granting another person access to an area, are responsible for that person's activities.

Media and hardcopy protection and transportation

- Printed versions of confidential data should not be copied or left unattended and open to unauthorized access.
- Media containing client-identified data will not be shared with any agency other than the owner of the data for any reason. HC HMIS data may be transported by authorized employees using methods deemed appropriate by the participating agency and that meet the above standard. Reasonable care should be used, and media should be secured when left unattended.
- Magnetic media containing HC HMIS data which is released and/or disposed of from the Participating Agency and Central Server should first be processed to destroy any data residing on that media.

- Degaussing and overwriting are acceptable methods of destroying data.
- Responsible personnel must authorize the shipping and receiving of magnetic media, and appropriate records must be maintained.
- HC HMIS information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

P&P#: ACC 4.7	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Unique User ID and Password

Policy: Authorized users will be granted a unique user ID and password.

Standard:

- Each user will be required to enter a User ID with a Password in order to logon to the system.
- User ID and Passwords are to be assigned to individuals.
- The User ID will be the first initial and full last name of the user. If a user has a first initial and last name that is identical to a user already in the system, the User ID will be the first initial and last name plus the number 01.
- The Password must be no less than eight and no more than sixteen characters in length.
- The password must be alphanumeric.

Purpose: In order to ensure that only authorized users will be able to enter, modify or read data, unique User ID will be issued to every user.

Scope: System wide

Procedures:

- Discretionary Password Reset Initially each user will be given a password for one time use only. The first or reset password will be automatically generated by ServicePoint and will be issued to the User by the Site Technical Administrator. Passwords will be communicated in written or verbal form. The first time, temporary password can be communicated via email. HC HMIS staff is not available to agency staff to reset passwords. Only an Agency Administrator can reset a password.
- Forced Password Change (FPC): FPC will occur every forty-five days once a user account is issued. Passwords will expire and users will be prompted to enter a new password. Users may not use the same password consecutively, but may use the same password more than once.
- Unsuccessful logon: If a User unsuccessfully attempts to logon three times, the User ID will be "locked out", access permission revoked and unable to gain access until their password is reset in the manner stated above.

P&P#: ACC 4.8	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Right to Deny User and Participating Agencies' Access

Policy: Participating Agency or a user access may be suspended or revoked for suspected or actual violation of the security protocols.

Standard: Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access.

Purpose: To outline consequences for failing to adhere to information security protocols.

Scope: Participating Agency

Procedure:

1. All potential violations of any security protocols will be investigated.
2. Any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to; a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment and criminal prosecution.
3. Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.
4. All sanctions are imposed by the Harford County Department of Community Services.

P&P#: ACC 4.9	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Data Access Control

Policy: Agency Administrators at Participating Agencies and HC HMIS staff must monitor access to system software.

Standards: Agency Administrators at Participating Agencies and HC HMIS staff must regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access.

Agency Administrators at Participating Agencies and HC HMIS staff must implement discretionary access controls to limit access to HC HMIS information when available and technically feasible.

Participating Agencies and HC HMIS staff must audit all unauthorized accesses and attempts to access HC HMIS information. Participating Agencies and HC HMIS staff also must audit all off-campus accesses and attempts to access HC HMIS systems. Audit records shall be kept at least six months, and Site Technical Administrators and HC HMIS staff will regularly review the audit records for evidence of violations or system misuse.

Purpose: To indicate the standards and guidelines for data access control for the participating agency.

Scope: System wide

Guidelines:

- Access to computer terminals within restricted areas should be controlled through a password or through physical security measures.
- Each user should have a unique identification code.
- Each user's identity should be authenticated through an acceptable verification process.
- Passwords are the individual's responsibility, and users cannot share passwords.
- Users should be able to select and change their own passwords, and must do so at least every forty-five days. A password cannot be re-used until 2 password selections have expired.
- Passwords should not be able to be easily guessed or found in a dictionary. The password

format is alphanumeric.

- Any passwords written down should be securely stored and inaccessible to other persons. Users should **not** store passwords on a personal computer for easier log on.

P&P#: ACC 4.10	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Auditing: Monitoring, Violations and Exceptions

Policy: HC HMIS staff will monitor access to all systems that could potentially reveal a violation of information security protocols.

Standard: **Monitoring**

HC HMIS staff will monitor compliance with the data security standards.

Violations

Any exception to the data security policies and standards not approved by HC HMIS is a violation, and will be reviewed for appropriate disciplinary action that could include termination of employment or criminal prosecution.

Exceptions

All exceptions to these standards are to be requested in writing by the Executive Director of the Participating Agency and approved by the HC HMIS Management Team.

Purpose: To outline the standards and procedures on compliance with information security protocols and the process by which HC HMIS staff will monitor compliance with such policies.

Scope: System wide

Monitoring

- Monitoring compliance is the responsibility of HC HMIS.
- All users and custodians are obligated to report suspected instances of noncompliance.

Violations

- HC HMIS staff will review standards violations and recommend corrective and disciplinary actions.
- Users should report security violations to the Agency Administrator, or HC HMIS staff person as appropriate.

Exceptions

- Any authorized exception to this policy must be issued from the Harford County Department of Community Services and the Participating Agency's Executive Director.

P&P#: ACC 4.11	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Local Data Storage

Policy: Client records containing identifying information that are stored within the Participating Agency's local computers are the responsibility of the Participating Agency.

Standard: Participating Agencies should develop policies for the manipulation, custody and transmission of client-identified data sets.

Purpose: To delineate the responsibility that Participating Agencies have for client-identified data.

Scope: Participating Agencies

Procedure: A Participating Agency develops policies consistent with Information Security Policies outlined in this document regarding client-identifying information stored on local computers.

P&P#: ACC 4.12	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Transmission of Client Level Data

Policy: Client data will be transmitted in such a way as to protect client privacy and confidentiality.

Standards: Administrators of the Central Server data must be aware of access-control vulnerabilities for that data while they are in transmission within the network.

Purpose: To provide guidelines regarding security of client level data during transmission.

Scope: System wide

Guidelines: Transmission will be secured by 128-bit encryption provided by SSL Certificate protection, which is loaded at the HC HMIS server.

SECTION 5:

Technical Support and System Availability

P&P#: SUP 5.1	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Planned Technical Support

Policy: HC HMIS staff will offer technical support to all Participating Agencies.

Standard: HC HMIS staff will provide technical assistance to Participating Agencies on use of the system software.

Purpose: To describe the elements of the technical support package offered by HC HMIS staff.

Scope: System wide

Procedure: HC HMIS staff will assist agencies in:

- Start-up and implementation
- On-going technical assistance
- Training
- Technical assistance with report writing

P&P#: SUP 5.2	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Participating Agency Service Request

Policy: HC HMIS staff will respond to requests for services that arrive from the Agency's Executive Director or Agency Administrator.

Standard: To effectively respond to service requests, HC HMIS staff will require that proper communication channels be established and used at all times.

Purpose: To outline the proper methods of communicating a service request from a Participating Agency to HC HMIS staff.

Scope: Participating Agencies

Procedure:

Service Request from Participating Agency

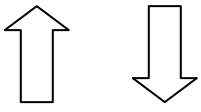
A. Agency Management Staff (Executive Director or Agency Administrator) contact assigned HC HMIS staff for service.

B. HC HMIS staff member determines the resources needed for service.

C. HC HMIS contacts agency management staff to work out a mutually convenient service schedule.

Chain of Communication

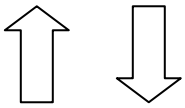
HC HMIS Staff



Agency Executive Director

Or

Agency Administrator



Agency Staff

P&P#: SUP 5.3	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Availability: Hours of System Operation

Policy: The system will be available to the community of users in a manner consistent with the user's reasonable usage requirements.

Standard: Members of the HC HMIS staff agree to minimally operate the system web site twenty hours a day/ seven days a week. Some time is required each day to backup the server and database.

Purpose: To delineate the schedule that HC HMIS staff will apply to make the system available to the network of users throughout Harford County.

Scope: System wide

Schedule: The system will be available from 6:00 A.M-12:00 PM and 2:00PM- 4:00AM, seven days a week, excluding acts of god, or federal or state declared emergency situations.

P&P#: SUP 5.4	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Availability: HC HMIS Staff Availability

Policy: HC HMIS staff will be available to the community of users in a manner consistent with the user's reasonable service request requirements.

Standard: HC HMIS staff are available for Technical Assistance, questions, and troubleshooting between the hours of 8:30 and 5:00 Monday to Friday, excluding County and federal holidays.

Purpose: To delineate the range of issues that HC HMIS staff will be available to resolve technical issues.

Scope: System wide

Procedure:

P&P#: SUP 5.5	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Title: AVAILABILITY: PLANNED INTERRUPTION TO SERVICE

Policy: HC HMIS staff will inform Participating Agencies of any planned interruption to service.

Standard: Participating Agencies will be notified of planned interruption to service one week prior to the interruption.

Purpose: To indicate procedures for communicating interruption to service. To indicate procedures for communicating when services resume

Scope: System-wide

Procedure:

Planned Interruption to Service

HC HMIS staff will notify Participating Agencies via e-mail and/or fax the schedule for the interruption to service. An explanation of the need for the interruption will be provided and expected benefits or consequences articulated.

Service Restoration

HC HMIS staff will notify via e-mail and/or fax that service has resumed.

P&P#: SUP 5.6	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Availability: Unplanned Interruption to Service

Policy: Participating Agencies may or may not be notified in advance of unplanned interruption to service.

Standard: Participating Agencies will be notified of unforeseen interruption to service that are expected to exceed two hours.

Purpose: To indicate procedures for communicating unforeseen interruption to service.

Scope: System wide

Unplanned Interruption to Service

When an event occurs that makes the system inaccessible HC HMIS staff will notify Participating Agencies via e-mail and/or fax that service has resumed.

SECTION 6:

Data Release Protocols

P&P#: SUP 6.1	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Data Release Authorization and Distribution

Policy: HC HMIS staff will follow Community Services procedures for the release of all data.

Standard: HC HMIS staff will abide by Access to Data Policies as established by Community Services.

Purpose: To outline the procedures for the release of data from the HC HMIS Project.

Scope: HC HMIS staff

Procedure: All data that are to be released in aggregate format must represent at least sixty percent (60%) of the clients in that region.

Release of data principals (Participating Agency)

- Only de-identified aggregate data will be released.
- Program specific information will not be released without the written consent of the Participating Agency Executive Director.
- There will be full access to aggregate data for the inner circle (all participating agencies).
- Aggregate data will be available in the form of an aggregate report or as a raw data set.
- Aggregate data will be made directly available to the public in the future.
- Parameters of the aggregate data, that is, where the data comes from, what it includes and what it does not include will be presented with each report.
- Community Services Director or Deputy Director will analyze the situation and make decisions when approval is required for release of data that do not meet the 60% release rate.

P&P#: DAT 6.2	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Right to Deny Access to Client Identified Information

Policy: HC HMIS retains authority to deny access to all client identified information contained within the system.

Standard: No data will be released to any person, agency, or organization that is not the owner of said data.

Purpose: To protect client confidentiality

Scope: System wide

Procedure:

1. Any request for client identified data from any person, agency, or organization other than the owner will be forwarded to the Harford County Review Board for review.
2. Pursuant to Harford County Review Board Policy any outside entity must obtain the written consent of every client contained within the database prior to the release of the data.

P&P#: DAT 6.3	**Revision:**	**Prepared by: HC HMIS**
Effective date: 05/04	**Revision date:**	**Revised by:**

Right to Deny Access to Aggregate Information

Policy: HC HMIS staff retain authority to deny access to all aggregate data contained within the system.

Standard: No data will be released without proper authorization

Purpose: To prevent the unauthorized distribution of aggregated reports.

Scope: System wide

Procedure: When a person or organization requests data, the request will be reviewed by the Harford County Department of Community Services.

ATTACHMENTS

Attachment 1

Harford County

Homeless Continuum of Care

Harford County HMIS Agency/End User Agreement

This contractual agreement is entered into on ___ /___ /___ between the **HC HMIS Project,** and

Agency Name: _____

Executive Director: _____

Name of staff person receiving an HMIS user license: _____
Agency

Address: _____ Phone: (____)_____-_____
_____ Fax: (____)_____-_____
_____ Email: _____

This document contains the specific obligations that each agency, including all agency staff persons receiving a user license, and Harford County Community Services must follow in order to participate in the HC HMIS Project. The signatories for this document shall be the Agency Executive Director or designee and the agency staff person receiving a user license.

I. Contractual Requirements and Roles

_____
Signature

I agree to abide by all policies and procedures contained in **Section 1** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **Steering Committee:** Advises the project on activities.

B. **Participating Agency Executive Director**: Assumes responsibility for the entire implementation and administration of the system

C. **Participating Agency Administrator**: The Executive Director's designees to manage operations.

D. **Participating Agency User**: Agency Staff who serve clients who are authorized by the Executive Director to access the system.

E. **Contractual compliance** with all elements of the Harford County, End User and Taxonomy, Business Associate Agreements, as well as the User License Policy, Responsibility & Confidentiality Statement. (Attachments 2,3,4 & 5).

II. Participation Requirements

_____
Signature

I agree to abide by all policies and procedures contained in **Section 2** of the HC HMIS Policies and

Procedures including but not limited to the following policies as listed below.

A. **Participation Requirements of Participating Agency and HC HMIS:** Lays out responsibilities of all parties involved in implementation.

B. **Implementation Documentation:** Delineates all written documentation required for implementation including data sharing agreements, client consent forms, data collection commitment and participating agency security protocols.

C. **Minimal Data Elements**: Participating agencies must make every effort to enter information on all clients served in participating programs. Agencies agree to enter at a minimum, all universal data elements and program specific data elements if the agency provides case management.

D. **Confidentiality**: The Participating Agency will uphold Federal and State Confidentiality regulations that protect client records and privacy as referenced in 42 CFR Part 2, Health Insurance Portability and Accountability Act (HIPPA) and State of Maryland Code, Health - General, Title 4, Statistics and Records, Subtitle 3 Confidentiality of Medical Records and the HUD HMIS Data and Technical Standards Final Notice in the Federal Register 7/30/04 issue.

E. **Maintenance of Internet Connection and Onsite Computer Equipment:** Outlines responsibility of agency in maintaining connectivity and equipment.

III. Training

_____

Signature

I agree to abide by all policies and procedures contained in **Section 3** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **Training Schedule**: HC HMIS staff will provide schedule and on site training as documented.

B. **User, Administration and Security Training**: Prior to being granted access to the system, all staff will be trained on relevant information security issues.

IV. User, Location, Physical, and Data Access

_____

Signature

I agree to abide by all policies and procedures contained in **Section 4** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **User Access**: Identifies process for user access including authorization of user names and passwords

B. **Location Access**: Participating agencies must identify the locations from which system software can be accessed.

C. **Physical Access**: All agencies must develop internal access policies to all systems.

D. **Data Storage and Transmission**: All agencies will develop internal protocols for the transmission and storage of client level information. HC HMIS staff are available to provide recommendations for policy development.

V. Technical Support and System Availability

_____

Signature

I agree to abide by all policies and procedures contained in **Section 5** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **Planned Technical Support:** Participating agencies will receive planned technical support as requested.

B. Availability: System software will be made available for set periods of time with time allowed for updates and protocols for unplanned interruption to service.

VI. Data Release Protocols

_____

Signature

I agree to abide by all policies and procedures contained in **Section 6** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **Data Release Authorization:** Outlines specific policies regarding release of aggregate data.

By signing this document, I agree to abide by all policies as stated in the HC HMIS Policies and Procedures Document. I also agree to educate all staff members in my agency as to the policies that directly affect their work.

Name of Program _____

Name of Sponsoring Agency _____

Name/Title of Person Receiving

An HMIS User License _____

_____

Agency Staff End User _____ _____

Signature of Person Receiving License Date

Executive Director _____ _____

Signature of Executive Director Date

HC HMIS Staff Person _____ _____

Signature of HC HMIS Staff Person Date

Attachment 2

Contract

ServicePoint™ License and Service Agreement

This agreement made and executed this the 12th day of March, 2004, between Bowman Internet Systems LLC (hereinafter referred to as "BIS"), 333 Texas Street, Suite 300, Shreveport, Louisiana 71101 and Harford County, Maryland, (hereinafter referred to as "CLIENT" or "you") with a permanent address of 220 S. Main Street, Bel Air, Maryland 21014

WHEREAS, CLIENT agrees to obtain from BIS, and BIS, by its execution of this agreement, agrees to furnish CLIENT under the terms and conditions contained herein, the Services detailed in the 'Pricing Table' of this proposal;

NOW, THEREFORE, in consideration of the premises and in further consideration of the performance of the terms and provisions herein contained, BIS and CLIENT do hereby contract and agree as follows:

(1) Term. CLIENT agrees to the contract for the length of 12 months, beginning upon acceptance of this agreement by signature, with a renewal term of 12 months at the same terms and conditions. This agreement will automatically renew for successive 12-month periods unless cancelled or modified within thirty (30) days of the end of the term. Any modifications must be submitted in writing to the other party and agreed to by the other party.

(2) Services. BIS will provide Intranet programming, implementation, and hosting services for CLIENT to include services listed in and according to the specifications set forth in the 'Pricing Table' of proposal.

(3) Fees. CLIENT agrees to pay BIS the fees, payments and expenses set out in 'Pricing Table' of the proposal dated 1/31/03, for the creation and implementation of intranet program described in said 'Pricing Table' of proposal, payment terms are listed in the 'Pricing Table' of proposal. All additional user licenses purchased for the system during the term of this contract will be available at the rate specified in the 'Pricing Table; $175.00 per 1/03 Price List attached.

(4) Warranties. In the event of loss of data due to errors and/or negligence on the part of BIS, BIS will correct program error in a timely fashion at no additional cost to CLIENT. Other than herein above described, BIS makes no express or implied warranties and makes no implied warranty of merchantability or fitness for a particular purpose. In no event shall BIS be liable for indirect, consequential, punitive or special damages. BIS shall not be responsible for loss of data resulting from

delays, non-deliveries, mis-deliveries, service interruptions, or other interruptions caused by CLIENT or any other person or entity, except Bowman Internet Systems.

(5) License. This agreement includes 1 server software license and (see pricing proposal) user licenses. The ServicePoint™ administration section will display the maximum number of users allowed. Individual agencies needing additional users can obtain additional user licenses by contacting authorized BIS representatives and payment for additional licenses. In addition, additional agency user licenses can be purchased at any time during the duration of this agreement for the agency user license fees listed in the 'Standard Pricing' of proposal.

a. **Server License.** One copy of a ServicePoint server license must accompany each server that CLIENT uses to utilize the ServicePoint program.

b. **User License.** Each user of the system must obtain a unique user license. Sharing of user names and passwords is expressly forbidden. In addition, each user of the system must agree to the End User License agreement located in Terms of Use in the program. The End User License Agreement is also attached to this agreement. ServicePoint users have a thirty-day refusal period to reject the End User License Agreement. If refused, the user must be denied access to the system and BIS will make a full user license refund.

c. **Third party licenses.** If CLIENT chooses to host ServicePoint™ on their network, additional third party licenses will apply, at the CLIENT's costs. Third party licenses include, but are not limited to Microsoft SQL, Microsoft Internet Information Server, PHP, and Microsoft Windows NT.

(6) Upgrades. This license includes routine system upgrades. Major version upgrades can be purchased on an as needed basis for upgrade fees set at the time of version release. However, no version upgrades are mandatory and additional purchases are at the discretion of CLIENT. BIS normally provides support options for the current and previous major release of ServicePoint. BIS reserves the right to terminate support for older versions upon six months advance written notice to CLIENT.

(7) Trade Secret. CLIENT hereby acknowledges that the source code related to services and products provided by BIS under this Agreement constitutes a trade secret of BIS, and as such is protected by civil and criminal law, is very valuable to BIS, and that its use must be carefully and continuously controlled. In accordance with the aforesaid, CLIENT agrees to use best efforts to ensure the confidentiality of the source code, and will prohibit the unauthorized access to, use or duplication of any of the source code. CLIENT agrees to keep all source codes in a secure environment, which is as secure as CLIENT provides for its most confidential materials. CLIENT will not cause, permit, nor allow the code or materials provided by BIS to be copied, duplicated, transcribed, sold to, revealed to, or used by any other person, firm or company without prior written consent of BIS. CLIENT agrees to notify BIS immediately of the unauthorized possession, use or knowledge of any item

supplied under this Agreement by any person or organization not authorized by this Agreement to have such possession, use or knowledge, and will cooperate fully with BIS in any litigation against third parties deemed necessary by BIS to protect its proprietary rights. CLIENT'S compliance with the above shall not be construed in any way as a waiver of BIS's right to recover damages or obtain other relief against CLIENT for its negligent or intentional harm to BIS's proprietary rights or for breach of contractual rights. If CLIENT attempts or allows others to attempt to use, copy, duplicate, transcribe, or convey the items supplied by BIS pursuant to this Agreement, in a manner contrary to the terms of this Agreement or in derogation of BIS proprietary rights, whether these rights are explicitly herein stated, determined by law, or otherwise, BIS shall have, in addition to any other remedies available to it at law or equity, the right to injunctive relief enjoining such actions, CLIENT hereby acknowledging that irreparable harm will occur to BIS and that other remedies are inadequate.

(8) Compliance with Laws. CLIENT assumes all responsibility in assuring compliance with all regulations relating to CLIENT's use of the product and services.

(9) Confidentiality. BIS and CLIENT each agree that all information pertaining to the terms and conditions of this Agreement and CLIENT Proposal, whether before the effective date or during the term of this Agreement, shall be received in strict confidence, and that such information shall be disclosed by the recipient party, its agents or employees only as required by Maryland Public Information Act, unless such information is publicly available from other than a breach of these provisions. Each party agrees to take all reasonable precautions to prevent the disclosure to outside parties of such information, except as may be necessary by reason of legal, accounting or regulatory requirement beyond the reasonable control of BIS and CLIENT, as the case may be. BIS agrees that all information input into the program is deemed confidential, and that no such information shall be disclosed by BIS to any outside party, unless such information is publicly available from other than a breach of these provisions. BIS agrees to take all reasonable precautions to prevent the disclosure to outside parties of such information, except as may be necessary by reason of legal, accounting, or regulatory requirement beyond the reasonable control of BIS, as the case may be.

(10) Delivery. Delivery of Services described in the 'Pricing Table' has been projected to occur 30 working days after the contract signing and upon full payment.

(11) Use of Server. BIS will host CLIENT's Intranet application on a server on BIS's network. The server, its components, and its software are property of BIS. However, data input by CLIENT is property of CLIENT. BIS's server may not be used for illegal purposes, or in support of illegal activities. Activities which are prohibited as potentially illegal include, but are not limited to unauthorized copying of material, transmittal of chain letters, threatening bodily harm or property damage of individual groups, making fraudulent offers of products, items, or services originating from your account, attempting to access the accounts of others or attempting to penetrate our

systems whether or not the intrusion results in loss of data, or distributing viruses or bulk e-mail through the BIS system.

(12) Modification. CLIENT may not modify source code without written consent of BIS.

(13) Statute of Limitations. No action arising out of this Agreement may be brought by CLIENT or BIS more than one (1) year after the cause of action has occurred, and the injured party has actual knowledge of the occurrence.

(14) Complete Agreement. This document contains the entire agreement between the parties with respect to the transactions contained herein and supersedes all prior proposals and understandings, both oral and written. This Agreement may be modified or altered only by a written instrument signed by all parties hereto.

(15) Headings. The headings of each paragraph contained herein are provided only for convenience and shall not be deemed controlling.

(16) Binding. This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective assigns and successors.

(17) Assignability. This Agreement shall not be transferable or assignable by CLIENT or BIS without written consent by the other party. However, CLIENT or BIS may assign its rights and obligations under this agreement by written document, to which BIS and CLIENT consent in their reasonable discretion. In this event, the assignee shall be solely responsible and liable to the other party for the performance of the obligations and duties pursuant to this agreement. Also, in the event that BIS transfers or assigns the Agreement, no option to renegotiate this agreement with assignee shall occur and the assignee shall be bound by the terms and conditions herein for the balance of the term.

(18) Governing Law. This Agreement shall be governed by, construed, and enforced under, and subject to, the laws of the State of Maryland. If any of the provisions of this Agreement are invalid under any applicable statute or rule of law, they are, to that extent, deemed omitted. Such omission does not change the intent or binding nature of any or all of the rest of this Agreement, which shall be in full force and effect.

(19) Limitation of Liability. In the event of loss of data due to errors and/or negligence on the part of BIS, BIS will correct the program error in a timely fashion at no additional cost to CLIENT. Other than as herein above described, BIS shall in no event have any liability to CLIENT for losses sustained or liabilities incurred except as may result from gross negligence or willful misconduct. Further, any liability of BIS for any loss, damages, or costs hereunder shall be limited to the actual direct damages incurred by CLIENT, but in no event shall the aggregate of liability exceed the total fees paid by CLIENT to BIS under paragraph 2 above, nor shall any amount of liability include any direct, consequential, punitive or special damages incurred by CLIENT. BIS shall not be responsible for loss of data resulting from delays, non-

deliveries, mis-deliveries, service interruptions, or other interruptions caused by CLIENT.

(20) Force Majeure. BIS shall not be liable to CLIENT or any other person or entity for any loss or damage for delay in performance, or for nonperformance, due to causes not reasonably within its control, such as, but not limited to, an act of God, strike, lockout, or other industrial disturbance, act of the public enemy, war, blockade, public riot, public disaster, lightning, fire, storm, flood or other act of nature, explosion, judicial orders/decrees, governmental laws/regulations, governmental action, governmental delay, restraint or inaction, unavailability of equipment, and any other cause, whether of the kind specifically enumerated above or otherwise, which is not foreseeable or reasonably within the control of BIS.

(21) Notice. Any notices under this Agreement shall be written and shall be deemed delivered when actually received, or three days after they are deposited with the United States Postal Services, certified mail return receipt requested when addressed to the other party at its above address.

(22) Counterparts. Two (2) duplicate originals of this Agreement are executed with each party retaining one (1) copy.

(23) Severability. The invalidity of any one or more of the provisions of this Agreement shall not affect the remaining portions of this Agreement, and in case of any such invalidity, this Agreement shall be construed as if the invalid provisions had not been inserted.

(24) Termination for Convenience. The performance of work under this agreement may be terminated by the CLIENT in accordance with this clause in whole, or from time to time in part, whenever the CLIENT shall determine that such termination is in the best interest of the CLIENT. The CLIENT will pay all reasonable costs associated with this agreement that BIS has incurred up to the date of termination and all reasonable costs associated with termination of the agreement. However, BIS shell not be reimbursed for any anticipatory profits that have not been earned up to the date of termination. Should the CLIENT exercise its option to terminate its contract with BIS, BIS will cooperate with an HMIS vendor designated by the CLIENT to transfer CLIENT services provider data into the designated HMIS.

(25) Termination for Cause.

If BIS is adjudged as bankrupt, or if it makes a general assignment for the benefit of the creditors, or if a receiver is appointed on account of its insolvency, or if it persistently or repeatedly refuses or fails to comply with the terms and conditions of this agreement then the CLIENT, after certifying that sufficient cause exists to justify such action, may without prejudice to any right or remedy and after giving BIS seven (7) days written notice, terminate the agreement. Should the CLIENT exercise its option to terminate its

contract with BIS, BIS will cooperate with an HMIS vendor designated by the CLIENT to transfer CLIENT services provider data into the designated HMIS.

(27) Insurance.

a. Prior to the execution of the contract, the successful offer or must obtain, at its own cost and expense, and keep in full force and effect until termination of the contract, the following insurance, written in companies licensed to do business in the State of Maryland.

b. The coverage will be evidenced by a certificate of insurance issued directly to the County by the offertory's agent, and provide 60 days' written notice to the County of cancellation or material change in coverage. A two-year extended reporting provision is required to safeguard against gaps in coverage after policies are terminated. All liability policies shall name Harford County, Maryland as an additional insured.

c. Required Coverages and Limits:

.1	Automobile Liability (owned, hired and non-owned automobiles):	$1,000,000
	Bodily injury, person	$1,000,000
	Bodily injury, per occurrence	$1,000,000
	Property damage, per occurrence	$1,000,000
.2	Commercial General Liability:	$2,000,000
	Bodily injury, property damage or medical expenses, per occurrence:	$1,000,000
	Bodily injury, property damage and personal injury claims:	$1,000,000
.3	Workers Compensation:	Statutory limit

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed on the date first above written.

Bowman Internet Systems LLC
333 Texas Street, Suite 300
Shreveport, Louisiana 71101
(BIS)

WITNESS/ATTEST:

By: _____
Robert Bowman
President

Date: _____

WITNESS/ATTEST:

HARFORD COUNTY, MD.

_____

_____
Lucy Light Slaich
Director of Procurement
Secretary, Bd. of Estimates

Approved for form and legal sufficiency

Approved for financial sufficiency

_____
Deborah S. Duvall
Sr. Assistant County Attorney

_____
John R. Scotten, Jr.
Treasurer

_____
Mary Chance, Director
Director, Community Services

Approved by Harford County Board of Estimates September 25, 2003.

Attachment 3

Harford County
Homeless Continuum of Care

Harford County HMIS Agency/End User Agreement

This contractual agreement is entered into on ___ /___ /___ between the **HC HMIS Project,** and

Agency Name: _____

Executive Director: _____

Name of staff person receiving an HMIS user license: _____
Agency

Address: _____ Phone: (____)_____-_____
_____ Fax: (____)_____-_____
_____ Email: _____

This document contains the specific obligations that each agency, including all agency staff persons receiving a user license, and Harford County Community Services must follow in order to participate in the HC HMIS Project. The signatories for this document shall be the Agency Executive Director or designee and the agency staff person receiving a user license.

I. Contractual Requirements and Roles

_____
Signature

I agree to abide by all policies and procedures contained in **Section 1** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **Steering Committee:** Advises the project on activities.

B. **Participating Agency Executive Director**: Assumes responsibility for the entire implementation and administration of the system

C. **Participating Agency Administrator**: The Executive Director's designees to manage operations.

E. **Participating Agency User**: Agency Staff who serve clients who are authorized by the Executive Director to access the system.

E. **Contractual compliance** with all elements of the Harford County, End User and Taxonomy, Business Associate Agreements, as well as the User License Policy, Responsibility & Confidentiality Statement. (Attachments 2,3,4 & 5).

II. Participation Requirements

_____
Signature

I agree to abide by all policies and procedures contained in **Section 2** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **Participation Requirements of Participating Agency and HC HMIS:** Lays out responsibilities of all parties involved in implementation.

B. **Implementation Documentation:** Delineates all written documentation required for implementation including data sharing agreements, client consent forms, data collection commitment and participating agency security protocols.

C. **Minimal Data Elements**: Participating agencies must enter information on all clients served in participating programs. Agencies agree to enter at a minimum, all data universal data elements and program specific data elements if the agency provides case management.

D. **Confidentiality**: The Participating Agency will uphold Federal and State Confidentiality regulations that protect client records and privacy as referenced in 42 CFR Part 2, Health Insurance Portability and Accountability Act (HIPPA) and State of Maryland Code, Health - General, Title 4, Statistics and Records, Subtitle 3 Confidentiality of Medical Records and the HUD HMIS Data and Technical Standards Final Notice in the Federal Register 7/30/04 issue.

E. **Maintenance of Internet Connection and Onsite Computer Equipment:** Outlines responsibility of agency in maintaining connectivity and equipment.

III. Training

_____

Signature

I agree to abide by all policies and procedures contained in **Section 3** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **Training Schedule**: HC HMIS staff will provide schedule and onsite training as documented.

B. **User, Administration and Security Training**: Prior to being granted access to the system, all staff will be trained on relevant information security issues.

IV. User, Location, Physical, and Data Access

_____

Signature

I agree to abide by all policies and procedures contained in **Section 4** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **User Access**: Identifies process for user access including authorization of user names and passwords

B. **Location Access**: Participating agencies must identify the locations from which system software can be accessed.

C. **Physical Access**: All agencies must develop internal access policies to all systems.

D. **Data Storage and Transmission**: All agencies will develop internal protocols for the

transmission and storage of client level information. HC HMIS staff are available to provide recommendations for policy development.

V. Technical Support and System Availability

_____

Signature

I agree to abide by all policies and procedures contained in **Section 5** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **Planned Technical Support:** Participating agencies will receive planned technical support as requested.

B. Availability: System software will be made available for set periods of time with time allowed for updates and protocols for unplanned interruption to service.

VI. Data Release Protocols

_____

Signature

I agree to abide by all policies and procedures contained in **Section 6** of the HC HMIS Policies and Procedures including but not limited to the following policies as listed below.

A. **Data Release Authorization:** Outlines specific policies regarding release of aggregate data.

By signing this document, I agree to abide by all policies as stated in the HC HMIS Policies and Procedures Document. I also agree to educate all staff members in my agency as to the policies that directly affect their work.

Name of Program _____

Name of Sponsoring Agency _____

Name/Title of Person Receiving

An HMIS User License _____

Agency Staff End User _____ _____

Signature of Person Receiving License Date

Executive Director _____ _____

Signature of Executive Director Date

HC HMIS Staff Person _____ _____

Signature of HC HMIS Staff Person Date

Attachment 4

Department of Housing and Urban Development

Homeless Management Information Systems (HMIS);
Data and Technical Standards Final Notice

published in the

Federal Register Revised notice March 2010

Attachment 5

Harford County, Maryland
HMIS

Business Associate Agreement

This is an Agreement by and between the following parties (hereinafter the "Parties"): _____ (hereinafter the "Covered Entity") and Harford County, Maryland (hereinafter the "Business Associate").

Definitions

1. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualified as a personal representative in accordance with 45 CFR § 164.502(g).

2. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

3. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

4. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

5. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

6. Underlying Services Agreement. "Underlying Services Agreement" shall mean the agreement between Covered Entity and Business Associate by which Business Associate provides certain services to Covered Entity.

Obligations and Activities of Business Associate

1. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.

2. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

3. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business associate in violation of the requirement of this Agreement.

4. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware within two business days.

5. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from the Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

6. Business Associate agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of Protected Health Information received from the Covered Entity or created or received by Business Associate on behalf of Covered Entity available to the Covered Entity, or to the Secretary for purposes of the Secretary in determining Covered Entity's compliance with the Privacy Rule.

7. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

8. Business Associate agrees to provide to Covered Entity or an Individual, within five business days of receipt of a written request, information collected in accordance with Paragraph 7 above in order to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

A. Permitted Uses and Disclosures by Business Associate

1. Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to provide services to Covered Entity in accordance with the Underlying Services Agreement, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity.

2. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Term and Termination

1. The Term of this Agreement shall be effective as of Enter Effective Date, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity.

Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

a. Provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement and the Underlying Services Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

b. Immediately terminate this Agreement and the Underlying Services Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

c. If neither termination nor cures are feasible, Covered Entity shall report the violation to the Secretary.

d. In the event of a conflict between the termination provisions of the Business Associate Agreement and the Underlying Services Agreement, the provisions of this Business Associate Agreement shall govern.

e. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

f. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide Covered Entity notification of the conditions that make return or destruction infeasible. Upon agreement of the parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Insurance and Indemnification

1. Indemnification. Business Associate shall indemnify and hold harmless Covered Entity from and against any claim, cause of action, judgment, damages, penalties, fines or reasonable attorneys fees that arise from the use or disclosure by Business Associates of Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, in violation of the Privacy Rule.

Insurance. Independent Contractor shall maintain and provide certification of Insurance to cover the above Indemnification in the minimum amount of one million dollars ($1,000,000) for each incident and three million dollars ($3,000,000) for annual aggregate coverage. Such certification shall name Covered Entity as Certificate Holder and shall include the following provision:

"It is agreed that this policy is not subject to cancellation of or reduction in coverage until 30 days after prior written notice has been given to

Certificate Holder."

Such certification shall be sent to Covered Entity at the following address:

_____
_____
_____

Miscellaneous

1. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

Survival. The respective rights and obligations of Business Associate set forth in this Agreement shall survive the termination of this Agreement.

Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

Agreed, this _____ day of _____, 2004, by the undersigned:

Business Associate: Harford County, Maryland

_____ _____
Signature Date

_____ _____
Name and title Witness

Covered Entity: _____

_____ _____
Signature Date

_____	_____
Name and title	Witness

Attachment 6

Harford County Continuum of Care HMIS
USER LICENSE POLICY, RESPONSIBILITY & CONFIDENTIALITY STATEMENTS

Agency Name _____ User's Name _____

User ID (Assigned by HC HMIS or Agency Administrator) _____

Each user requires a unique username and password (to be kept private). Use of another user's account, username and password is grounds for immediate termination from the Harford County Continuum of Care Homeless Management Information System.
Your username and password give you access to the Harford County Homeless Management Information System. Initial each item below to indicate your understanding of the proper use of your username and password, and sign where indicated. Any failure to uphold the confidentiality standards set forth below is grounds for immediate termination from the Harford County Homeless Management Information System.
RESPONSIBILITY STATEMENTS
Relevant points regarding client confidentiality include:

_____ I understand that my username and password are for my use only.
_____ I understand that I must take all reasonable means to keep my password physically secure.
_____ I understand that the only individuals who can view HCHMIS Tracking information are authorized users and the clients to whom the information pertains.
_____ I understand that I may only view, obtain disclose, or use the database information that is necessary in performing my job.
_____ I understand that if I am logged into ServicePoint, and must leave the work area where my computer is located, I must log-off the system before leaving the work area. Failure to log-off appropriately may result in a breach of confidentiality and system security.
_____ I understand those hard copies HCHMISS Tracking information must be kept in a secure file.
_____ I understand that these rules apply to all users of the HCHMIS Tracking Systems whatever their work role of position.
_____ I understand that once the hard copies of HCHMIS Tracking information are no longer needed, they must be properly destroyed to maintain Confidentiality.
_____ I understand that if I notice or suspect a security breach, I must immediately contact HCHMIS at (410) 638-3389.
STATEMENT OF CONFIDENTIALITY

I AGREE TO MAINTAIN THE STRICT CONFIDENTIALITY OF INFORMATION OBTAINED THROUGH The Harford County Continuum of Care Homeless Management Information System. This information will be used only for the legitimate client services and administration of the above named agency. Any breach of confidentiality will result in immediate termination of participation in the HCHMIS client tracking system.

User's Signature _____ Date _____

Agency Director/
Supervisor Signature _____ Date _____

Please mail this form back to:
Harford County Department of Community Services Office of Transitional Services
319 S. Main St., Bel Air, MD 21014

Attachment 7

Harford County
Homeless Continuum of Care

Program Information

Please complete for each program in the agency that will be linking data to ServicePoint.

Agency Name:

Program Name: Date:

Address:

City: **State:** **Zip:**

Completed by: **Phone Number:**

Type of Program:
- ☐ Emergency Shelter
- ☐ Transitional Housing ☐ Permanent Supportive Housing
- Supportive Services Only
- ☐ Outreach
- ☐ Other: specify

Population Served: ☐ Individuals ☐ Families ☐ Both

Target Population (ex. Youth, Elders):

Capacity Information: Please use the following categories to identify the number of beds/slots in your program. Select only **one** category per bed(s)/slot(s).

 # Individual Beds: # Beds entered into your database:

Regular:
Winter:
Overflow:
HUD Funded:

Operating Year: From ___/___/_____ To ___/___/_____

Additional:

Explain:

 # *Family Units:*

DTA Funded:
Community Beds:
Additional:

Explain:

Service Programs

**Slots:**
HUD **Funded:**

Operating Year: From ___/___/_____ To ___/___/_____

Other:

Explain:

Attachment 8

Harford County
Homeless Continuum of Care

ServicePoint User Access Form

Program Name: _____ Agency Administrator: _____
Executive Director: _____

Staff Name	Access Level (see below)	Status (active/inactive)	Authorized by	Date
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

Agency Access Levels	Resource Specialist I	Resource Specialist II	Resource Specialist III	Volunteer	Agency Staff	Case Manager	Agency Admin.	Execut. Director
ClientPoint								
Profile				X	X	X	X	X
Employment						X	X	X
Residential History						X	X	X
Medical/ Addict.							X	X

Legal						**X**	**X**	**X**
Military						**X**	**X**	**X**
Case Notes						**X**	**X**	**X**
Worksheets					**X**	**X**	**X**	**X**
ServicePt								
Referrals				**X**	**X**	**X**	**X**	**X**
Check-in/out				**X**	**X**	**X**	**X**	**X**
Other services					**X**	**X**	**X**	**X**
ResourcePt	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
ShelterPoint				**X**	**X**	**X**	**X**	**X**
Reports						**X**	**X**	**X**
Admin.								
Add Users							**X**	**X**
Remove Users							**X**	**X**
Reset Password							**X**	**X**
Add Agency								
Edit Agency		X	X				**X**	**X**
Other options								

Attachment 9

Harford County
Homeless Continuum of Care
HC HMIS Project

Location Access Authorization

Please list the locations and users of each computer that should be registered with the HC HMIS server that can access the ServicePoint software system.

Location	Computer Description	Users of Computer	Registered with Server (HC HMIS staff only)

Attachment 10

Harford County
Homeless Continuum of Care
HC HMIS Project

Laptop and Off Site Installation Access Privileges to System Server Commitment Form

Security Agreement

This agreement is made between the HC HMIS Project, Harford County Community Services, and _____.

Agency Name

By signing this security agreement, I agree that I will not allow persons other than Agency authorized staff to use the laptop. I understand that I will only access the ServicePoint software from locations authorized by the agency as appropriate for entering data. I realize that if I access the ServicePoint software from an unauthorized agency location that I am putting the confidentiality of all of the clients served in this agency at risk.

By signing this document, I agree to abide by the above policies.

_____ _____

Staff name Date

_____ _____

Agency name Date

Attachment 11

Harford County
Homeless Continuum of Care
HC HMIS Project

HC HMIS Staff Commitment Form
Staff Security Agreement

This agreement is being made between the HC HMIS Project, Harford County Department of Community Services, and _____.

Staff name

By signing this security agreement, I am acknowledging the following:

Location Access

1) I will not allow persons other than HC HMIS staff persons to use any of the computer equipment in the HC HMIS office.

2) I will not allow any persons other than HC HMIS staff to view my computer screen while logged on to the HMIS.

Central Server Database Access

3) Any information that I receive from the HC HMIS Project will be completely stripped of identifying information about the client's entered into the HC HMIS database.

Site Level Access

4) I will not view any client identifying information about an agency's data.

5) If a problem arises at a site that requires me to view client identified information, the Agency Administrator will log onto the ServicePoint system from his/her designated location and I will advise the Agency Administrator as to the steps to resolve the problem from their site location.

6) As a staff member with the HC HMIS Project, I am obligated to hold all information that I learn about clients as confidential.

Dissemination of Data

7) Any unauthorized copying or dissemination of all or a portion of the HC HMIS client identifiable data is punishable by termination of employment; and may result in severe civil and criminal penalties and will be punishable to the maximum extent possible under the law.

8) All reports will be produced using only client ID numbers (not names) to assure that all

reporting information is de-identified.

9) Any copies of de-identified, aggregate reports that are produced under this contract are to be used only for CoC planning, reporting, evaluation as well as for program reporting, monitoring, evaluation, staff training and data quality monitoring and are not to be released to any party other than HC HMIS Project Staff, Community Development Review Board members and Participating Agencies.

10) Upon termination of my employment with the HC HMIS Project I will return all materials I have worked with including any copies of the HC HMIS data which I received on disk, and any other relevant equipment and materials I received from the HC HMIS project.

11) I will report to the HC HMIS Manager any data handling practices that appear to fall short of any standard above.

By signing this document, I agree to the terms above.

_____ _____

Staff Signature Date

Attachment 12

Harford County
Homeless Continuum of Care
HC HMIS

Interagency Data Sharing Agreement

The HC HMIS Project administers a computerized record keeping system that captures information about people experiencing homelessness, including their service needs. The system, ServicePoint, allows programs the ability to share information electronically about clients who have been entered into the software. Client level information can only be shared between agencies that have established an Interagency Sharing Agreement and have received written consent from particular clients agreeing to share their personal information with another agency. The agency receiving the written consent has the ability to "share" that client's information electronically through the ServicePoint system with a collaborating agency.

This process can benefit clients by eliminating duplicate intakes. Intake and exit interviews can be shared, with written consent, between **NAMES OF COLLABORATING AGENCIES**.

By establishing this agreement, the **NAMES OF COLLABORATING AGENCIES** agree that within the confines of the HC HMIS Project and ServicePoint software:

1) ServicePoint information in either paper or electronic form will never be shared outside of the originating agency without client written consent.

2) Client level information will only be shared electronically through the ServicePoint System with agencies the client has authorized to see their information.

3) Information that is shared with written consent will not be used to harm or deny any services to a client.

4) A violation of the above will result in immediate disciplinary action.

5) Information will be deleted from the system upon client request.

6) Clients have the right to request information about who has viewed or updated their ServicePoint record.

We at **NAMES OF COLLABORATING AGENCIES** establish this interagency sharing agreement so that our agencies will have the ability to share client level information electronically through the ServicePoint System. This agreement does not pertain to client level information that has not been entered into the ServicePoint system. This electronic sharing capability only provides us with a tool to share client level information. This tool will only be used when a client provides written consent to have his/her information shared. **NAMES OF COLLABORATING AGENCIES** also have an agreement with the HC HMIS Project and have completed security procedures regarding the protection and sharing of client data.

By signing this form, on behalf of our agencies, I authorize the HC HMIS Project to allow us the to share information between our agencies. We agree to follow all of the above policies to share information between our collaborating agencies.

We agree the share the following information (please check all that apply):

. ☐ Basic Client Profile Information

. ☐ Residential History

. ☐ Employment Skills / Income

. ☐ Military / Legal

. ☐ Case Management

. ☐ Other (Please Specify)

Agency 1 Agency 2

Printed Name of Executive Director Printed Name of Executive Director

Signature of Executive Director Signature of Executive Director

Date Date

Attachment 13

Harford County
Homeless Continuum of Care
HC HMIS Project

SAMPLE Client Consent Form

The HC HMIS Project administers a computerized record keeping system that captures information about people experiencing homelessness, including their service needs. The programs in the **AGENCY NAME** have decided to use HC HMIS as their data management tool to collect information on the clients they serve and the services they provide.

This process benefits because you will not have to complete an additional intake interview. Intake information can be shared, with your written consent, from your service program to the **COLLABORATING AGENCY**.

If you consent, we have the ability to share your intake information with the **COLLABORATING AGENCY** to be used for an initial intake assessment. You can choose to share all or part of the information that you have shared including basic demographic information, residential, employment skills/income, military/legal, service needs, goals and outcomes. Your information will be shared electronically via a secure, encrypted, web-based system to the agencies of your choice. This will not take place unless you provide written consent. No medical, mental health, or substance use history will be shared unless you provide express written consent below. Your record will be shared for a period of no greater than five years from today's date.

The information that you share with the **COLLABORATING AGENCY** will be used to help you access services that will help you obtain and maintain permanent housing. You can choose to have any information that you have shared deleted from the system at any time as well as request a document containing information about who has viewed or updated your ServicePoint record. The information that you provide, combined with that provided by others, will be used, without any identifying information, for reporting requirements and advocacy.

We here at **AGENCY NAME** have an interagency sharing agreement with the **COLLABORATING AGENCY** regarding clients that are served by both agencies. Both programs also have an agreement with the HC HMIS Project and have completed security procedures regarding the protection and sharing of client data.

I, _____ _____ ☐ CONSENT

(Participant Signature) (Date) ☐ DO NOT CONSENT

to have information (demographic, residential, employment, income, military, legal, services, and goals and outcomes) that I provided in intake interviews to staff at **AGENCY NAME** to be shared electronically with the **COLLABORATING AGENCY** using the HC HMIS Computerized Record Keeping System.

MEDICAL, MENTAL HEALTH and SUBSTANCE USE HISTORY SHARING AUTHORIZATION

I, _____ _____ ☐ CONSENT

☐

(Participant Signature) (Date) ☐ DO NOT CONSENT

to have information (medical, mental health, and substance use history) that I provided in intake interviews to staff at **AGENCY NAME** to be shared electronically with the **COLLABORATING AGENCY** using the HC HMIS Computerized Record Keeping System. Agencies are responsible for

being aware of HIPAA compliance when sharing. I understand that I may ask to have this information removed from the HC HMIS computerized record keeping system at any time in the future.

(Participant Signature) Date

(Staff Member Signature) Date

Attachment 14

Harford County
Homeless Continuum of Care
HC HMIS Project

Referral Agencies Please provide the top 15 referral agencies/program (including services provided) utilized each agency program for inclusion in ResourcePoint, the service directory component of ServicePoint. You will be contacted for verification of information prior to entry into ResourcePoint.